TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI
2€
NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
n. 166
HACKER JOURNAL
www.hackerjournal.it
PRIVACY
Mascheriamo il Sistema operativo
SECURITY
LA LEGGENDA DEL ROOTKIT SINOWAL
PEER TO PEER
CASCATE DI TORRENT CON SEEDBOX
MOBILE
METTI IL SITO SUL CELLULARE
YOUTUBE in HIGH DEFINITION
VIDEO HACKING
QUATTORD. ANNO 8 - N° 166 - 18/31 DICEMBRE 2008 - € 2,00
9 771594 577001 80166
WLF PUBLISHING

Anno 8 – N.166
18/31 dicembre 2008

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Qualche amichevole consiglio

"L'uomo deve salvare se stesso con i propri sforzi, nessuno puó fare per lui quello che egli deve fare per se stesso".
Buddha

Lo avete letto tante volte sulle pagine di Hacker Journal: la sicurezza parte dalla testa e dal proprio atteggiamento, non dagli strumenti utilizzati per realizzarla.
Puoi avere l'antivirus più aggiornato, il firewall più efficace o il sistema di crittazione più sicuro, ma se non usi la testa sarà tutto inutile. L'uso di connessioni di rete come il Bluetooth o il wi-fi hanno aumentato esponenzialmente i rischi.

Qualche mese fa stavo viaggiando sull'Eurostar tra Milano e Roma e ho notato, tra le connessioni Wi-Fi disponibili, una strana rete: "Wi-fi free Internet by Trenitalia". Prima di farmi prendere dalla smania di approfittare del collegamento gratuito ho chiesto informazioni al controllore. Non gli risultava che ci fosse alcuna rete gratuita attivata dalle ferrovie. È bastato poi muovermi lungo il treno per capire che si trattava semplicemente di qualcuno che con il proprio portatile aveva creato una rete "point-to-point" e che attendeva che i pesci abboccassero all'amo per accedere alle loro risorse condivise e analizzare il loro traffico.

Il trasferimento dati tra il laptop e il cellulare via Bluetooth è decisamente comodo e finalmente si possono evitare quei fastidiosi cavi. Bastano però programmi piuttosto semplici da recuperare come Blitzkrieg, BlueDiving o BlueBugger per far sì che un malintenzionato possa accedere alla nostra rubrica, alle nostre foto e ai file salvati sul telefonino (nessuno ha segnato sul cell il codice PIN del bancomat, vero?!).

È chiaro che non tutti dati sono sensibili e che non ha senso crittografare l'intero disco fisso o disattivare completamente qualunque forma di connessione radio. Le connessioni senza fili portano con sé una indiscutibile comodità d'uso, ma bisogna sempre attivarne la crittazione e, nel caso del bluetooth, l'invisibilità verso dispositivi non registrati.

Se pensi che le nostre parole siano inutile allarmismo prova a cercare termini come "bluetooth", "wi-fi" e "security" su Google. C'è molta documentazione anche in italiano...

La conoscenza è il primo fondamentale passo verso la sicurezza.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Ancora bagarre sulle leggi anti-P2P

In realtà sono anni che se ne parla, che giunte parlamentari nazionali ed europee si combattono a suon di decreti e votazioni, ma la confusione continua a regnare sovrana fatta eccezione per qualche voce che balza subito all'orecchio (vedi Sarcozy e, poche settimane fa, Bush negli USA).

Qualche mese fa gli Europarlamentari hanno votato alcune modifiche alla legge denominata "Paquet Télécom" e palesemente appoggiata dalle major discografiche e cinematografiche.
Secondo queste modifiche (ormai conosciute semplicemente come "emendamento 138") nessuna restrizione alle libertà degli utenti può essere imposta, salvo il caso di forza maggiore o per conservare la sicurezza della rete, se non da un tribunale. Di fatto, quindi, questo emendamento proibirebbe i controlli e i provvedimenti a carico degli utenti scoperti a condividere materiale protetto da copyright se compiuti dai provider stessi e non dalle forze dell'ordine e dietro mandato del tribunale.
"Nulla può giustificare l'accaduto, trattandosi di norma fondamentale non solo sui diritti dei cittadini ma per l'intero comparto giuridico comunitario", dice uno degli autori dell'emendamento; "evidentemente il motivo deve ricercarsi nel progetto di legge francese contrario a quei principi".
Naturalmente, questo emendamento ha avuto vita breve, anche se in effetti la legge sulle telecomunicazioni ancora non è definita e il suo iter appare ancora lungo e laborioso.
Probabilmente, si pensa, è stata proprio il progetto di legge appoggiato da Sarcozy che, anche se ampiamente contestata dal pubblico e dagli stessi provider, ha trascinato nella stessa direzione il parlamento europeo.
Proprio per questo motivo Guy Bono, l'autore dell'emendamento 138 insieme al collega Daniel Cohn Bendit, ha intenzione di ripresentarlo in occasione della seconda consultazione in materia, prevista nel corso dei primi mesi del 2009.
Nell'ambiente però gli animi sono piuttosto pessimisti, malgrado l'entusiasmo di Bono.
C'è addirittura chi tira in ballo le leggi di Murphy: se una cosa può andare bene o male, sicuramente andrà male.
Noi speriamo sinceramente di no.

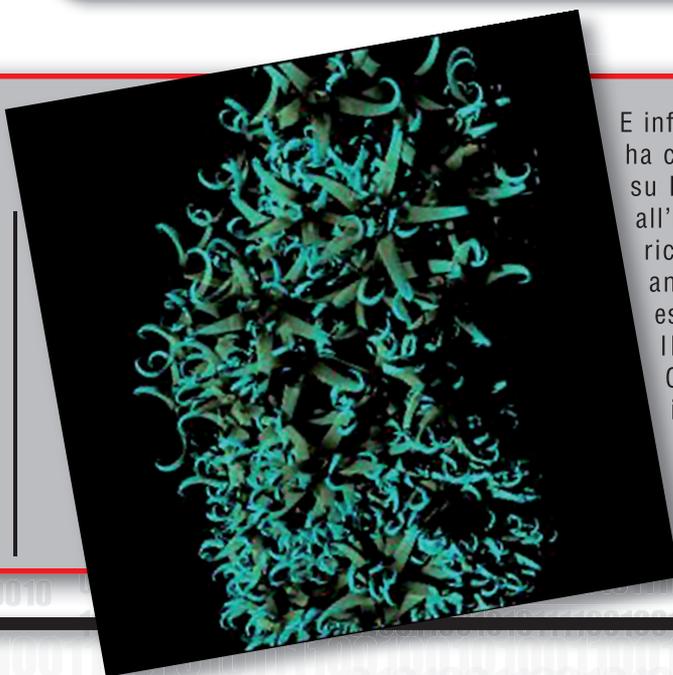
A CACCIA DI TERREMOTI

A Grottaminarda, località dell'Irpinia da sempre flagellata dai terremoti, è nato recentemente un nuovo osservatorio dell'Istituto Nazionale di Geofisica e Vulcanologia, con lo scopo di monitorare quella zona degli Appennini sita in un'area ad alto rischio sismico. L'obiettivo principale dell'osservatorio è quello di contribuire alla ricerca sui terremoti, con la speranza, un giorno, di poterli prevedere con precisione e per tempo. Inoltre in questa sede sono disponibili apparati per la magnometria: con essi è possibile sondare il terreno alla ricerca di grandi oggetti metallici sotterrati, per individuare e debellare discariche abusive e pericolose. Il centro si trova all'interno del Castello D'Aquino, un importante edificio storico.

SCATTI D'AUTORE DAL WEB

Si è tenuta nei primi giorni di dicembre a Lucca la seconda edizione di Scatti dal Web, una mostra fotografica promossa dalla comunità online MicroMosso.com con lo scopo di aggregare i membri, che così hanno potuto incontrarsi e conoscersi anche di persona, lasciando da parte per una volta la virtualità del Web. Sono stati 76 gli espositori, fotografi per professione o per passione. Le foto hanno spaziato tra argomenti diversi, senza un tema centrale, e sono già apparse nelle gallerie di MicroMosso.com nel corso di quest'anno. La comunità online vanta oltre 500 iscritti e ci si può iscrivere gratuitamente. Il successo avuto dalla manifestazione ha gettato già le basi per la prossima edizione, a cui tutti gli appassionati sono invitati.

IL WORM CHE TI CURA

In un post sul suo blog (http://blogs.technet.com/feliciano_intini/) Feliciano Intini, chief security advisor di Microsoft Italia aveva predetto che presto o tardi qualcuno avrebbe sfruttato una vulnerabilità di sicurezza di Windows contenuta nel servizio Server di Windows 2000, XP, Vista e Server 2003/2008, scoperta recentemente e corretta da Microsoft il 23 ottobre.

E infatti il worm Conficker.A ha cominciato a diffondersi su Internet, principalmente all'interno di aziende americane ma con apparizioni anche in Europa, Ucraina esclusa chissà perché...
Il fatto curioso è che Conficker.A, una volta installato vada correggere il bug di sistema per impedire che altri worm possano seguirne la sua strada.

SOCIAL NETWORK PER BELLI

È arrivato anche in Italia un nuovo modello di social networking. Per essere ammessi al sito, infatti, non basta registrarsi e compilare un profilo, ma si deve sostenere il giudizio degli altri iscritti del sesso opposto. Dopo tre giorni "in prova", se il proprio profilo ha ottenuto la maggioranza di voti positivi si entra di diritto nel network, altrimenti si viene definitivamente esclusi. Nulla vieta però, in un secondo momento, di provarci di nuovo, con una foto migliore e un profilo più interessante. Lo scopo BeautifulPeople.net (questo il nome del sito) è quello di offrire agli iscritti solamente il meglio della scelta. Ma Sgarbi avvisa: "anche il brutto serve, se non altro per esaltare il bello..."

PANINI CON COPYRIGHT

Parliamo di nuovo di brevetti, perché questo ha dell'incredibile. Tutti prima o poi ci siamo preparati un panino in cucina, in preda ai crampi della fame e con poco tempo per preparare qualcosa. Ma ora saremo tutti a rischio: il "metodo e apparecchiatura per preparare un sandwich" sono brevetti di proprietà di McDonalds! A parte l'apparecchiatura, che nel caso della nota azienda di fast food può essere anche plausibile, è il principio secondo cui il metodo stesso per preparare un panino, lo stesso da secoli, possa essere proprietà di qualcuno che ne abbia l'esclusiva. Il documento che descrive il brevetto contiene tanto di flowchart che spiega il processo, identico naturalmente a quello che useremmo noi in casa nostra. Non rimane che consolarci con la

USATO A RUBA

Molti utenti che hanno acquistato un nuovo PC con Windows Vista hanno poi venduto o messo all'asta su eBay il vecchio PC con Windows XP. Fin qui niente di strano. Il fatto è che pare proprio che questi PC usati stiano andando letteralmente a ruba: il motivo sarebbe la presenza della regolare licenza di Windows XP su questi vecchi computer, praticamente oro che cola per chi deluso da Vista vuole tornare a XP ma non può avvalersi delle facilitazioni di downgrade proposte da Microsoft. Questo sta portando anche a un aumento delle copie pirata di XP in circolazione, spesso anche piazzate su computer assemblati dai venditori. Comunque un'altra batosta per Vista, che a quanto pare proprio non lascerà un buon ricordo di sé all'arrivo di Windows 7.

E lo spam ritorna

Non abbiamo fatto in tempo a dare la notizia della incredibile diminuzione dell'odiato spam grazie all'individuazione di McColo (HJ 165) che l'attività degli spammatori ha ripreso a funzionare a pieno regime come testimonia il senior

anti-spam technologist di MessageLabs (http://www.messagelabs.com/) Matt Sergeant: "Le botnet dietro Asprox e Rustock sono tornate a colpire con violenza dopo aver individuato un nuovo centro di comando&controllo".

NOTEBOOK DUAL BRAND

Secondo le informazioni rilasciate da Digi-Times i prossimi notebook professionali Dell, e più precisamente i Latitude E4200 ed E4300 saranno equipaggiati da due processori. E fin qui niente di eccezionale. Sì, se non fosse che le due CPU saranno una Intel e l'altra basata su microarchitettura ARM. L'idea sarebbe quella di dotare il notebook di un'interfaccia minimalista stile netbook utilizzando il processore ARM per i compiti più essenziali quali mail, calendario, Internet, contatti e webcam mentre l'Intel viene tenuto di riserva per i compiti più gravosi.
Tutto ciò permetterebbe di aumentare notevolmente l'autonomia del portatile. Interessante vero? Ma armiamoci di pazienza, lancio ufficiale e prezzi non sono ancora stati comunicati.

IL PINGUINO CONQUISTA IPHONE

L'iPhone-Dev team ha messo una nuova tacca ai sistemi di sblocco per iPhone di cui vanta i maggiori successi. Ultimo in ordine di tempo il nuovo bootloader "openiboot" (e come poteva chiamarsi altrimenti?) che permette di caricare il kernel di Linux sullo smartphone di Mr. Jobs. In realtà si tratta più che altro di un esercizio di stile, una prova di muscoli per far vedere che "si - può - fareee!!". Il kernel infatti mette a disposizione una console con comandi limitati e sostanzialmente non consente di utilizzare le principali caratteristiche di iPhone come, ad esempio, il touchscreen o la connettività, né la possibilità di scrivere sulla memoria flash. E allora perché farlo? ma perché siamo hacker

GMAIL SICURA

Di tanto in tanto ritorna "una vulnerabilità di Gmail permetterebbe a malintenzionati di carpire i nostri domini". Recentemente è rimbalzata la voce secondo cui la falla del 2007 mietesse ancora vittime, ma Google ha smentito con decisione rassicurando i propri utenti: non si tratterebbe di falle di sistema ma (incredibile) più semplicemente di classico phishing. Nel caso specifico sarebbe un dominio del tipo "google-host.com". Una volta ottenuta con l'inganno la password, ai truffatori è sufficiente introdursi nell'account e impostare un filtro che inoltri a un proprio indirizzo tutte le email desiderate.

APRILE APRE IN VISTA

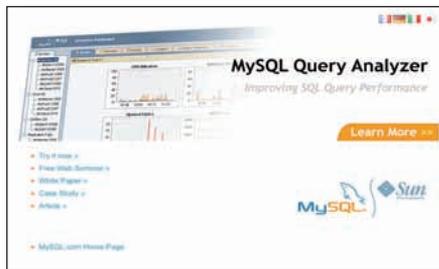
Secondo alcune indiscrezioni ad aprile vedrà la luce il Service Pack 2 di Windows Vista. In realtà la versione che potremo testare questa primavera sarà solo la

HOT NEWS

LA SICUREZZA VIAGGIA VIA SMS

È iniziata in via sperimentale in alcuni Paesi, ma se i risultati saranno soddisfacenti sarà allargata al resto del mondo. Stiamo parlando dell'iniziativa di PayPal, il sistema di pagamento di proprietà di eBay largamente utilizzato da tutti i principali siti di e-commerce, che per difendere la sicurezza dei propri utenti ha adottato un sistema (opzionale) che sfrutta l'invio di un codice di sicurezza via sms. In breve l'utente che ha effettuato un acquisto con PayPal, una volta effettuato il login inserendo i propri account e password , riceve via sms un codice di 6 cifre da digitare nell'apposita finestra. Questo ulteriore livello di sicurezza è gratuito dal lato PayPal ma eventuali costi potrebbero essere addebitati dal proprio operatore di telefonia mobile e chissà perché abbiamo l'impressione che in Italia qualche cen-

PRESENTATO MYSQL 5.1

È stata annunciata da parte di Sun la distribuzione della nuova versione 5.1 del popolare database open source MySQL. La nuova release integra aggiornamenti quali la partizione della tabelle, il supporto per la replicazione in linea e un nuovo plugin per le API. Fin qui nulla di nuovo, sembrerebbe la classica evoluzione di apprezzato software. Se non fosse che proprio il suo creatore, Michael Widenius, mette sul chi vive la comunità degli sviluppatori sulla presenza di "ben 20 bug critici che portano a crash e risultati errati, e di altri 35 che erano già presenti nella versione precedente, e che probabilmente ci sono ancora". La sua critica prende però di mira più che altro la scelta di aver etichettato la versione come "Generally Available" e incolpa direttamente Marten Mickos, vicepresidente di Sun e ex CEO di MySQL AB, e la sua strategia. Forse che forse la sparata di Widenius nasconde una guerra intestina?

BARO ON LINE

Sta prendendo sempre più piede la mania del video poker, aiutata da trasmissioni televisive e quintalate di pubblicità sui media. In realtà non tutti sanno che il gioco del poker d'azzardo è vietato nella gran parte dei paesi del mondo, soprattutto in USA e in Europa. Tuttavia, grazie alla "libertà" di Internet, i siti per giocare online che si appoggiano su server installati in zone franche stanno trasformando (e rovinando) le vite di molte persone. Come Russ Hamilton, ex campione di poker che, si è recentemente scoperto, è un ex dipendente di una di queste società e che ha sempre barato, preparandosi un programma per sapere sempre le carte in mano agli avversari in tempo reale. A scovarlo, alcuni incalliti giocatori, ex legali (ma quanti ex!) e improvvisati detective. Se non volete diventare anche voi ex...

"Release To Manufacturing" ma l'attesa è comunque grande anche perché le novità saranno tante e interessanti: Windows Search 4.0, che aumenterà la velocità di ricerca dei file, avrà il supporto Bluetooth 2.1, supporterà la masterizzazione su Blu-Ray e ultimo ma non ultimo Windows Connect Now (WCN) per semplificare la configurazione Wi-Fi. Correggerà anche il problema del riavvio per chi usa un PC con due processori, introdotto dal Service Pack 1.

CHROME APRE AGLI INDIPENDENTI

Vi ricordate di Chrome? Solo qualche mese fa sembrava dovesse essere la grande novità informatica del 2008; tremate tremate arriva il browser di Google. Lanciato in fretta e furia (come abbiamo spiegato su hj 163) oggi pare che il colosso di Moutain View abbia deciso di seguire la strada di Firefox, aprendo le porte agli sviluppatori indipendenti per incorporare le numerose estensioni che hanno fatto la fortuna del browser più amato della rete. Sul sito di Chromium (http://code.google.com/chromium/) troviamo la prima documentazione per gli sviluppatori.

Ecco cosa ci propone la tecnologia per la nostra sicurezza

TUTTO SOTTO CONTROLLO

Dal 25 al 28 novembre si è tenuta presso il moderno polo fieristico di Rho-Pero, nei pressi di Milano, l'edizione 2008 di Sicurezza e di Sicurtech. Si tratta di due esposizioni internazionali, principalmente per gli operatori del settore, che riguardano le tecnologie per la sicurezza a tutti i livelli, da quella personale e domestica a quella sul lavoro, per arrivare fino alle forze dell'ordine, alla protezione civile e al soccorso pubblico. Anche se alcuni di questi settori possono sembrare un po' al di fuori degli argomenti trattati normalmente su queste pagine, in realtà si è trattata di una giornata interessante avendo toccato con mano quanto l'informatica sia sempre più presente nel quotidiano e quanto la sicurezza in generale stia diventando un argomento di vitale importanza, sempre più al centro degli studi e delle preoccupazioni di tutti.

:: Sicurezza del territorio

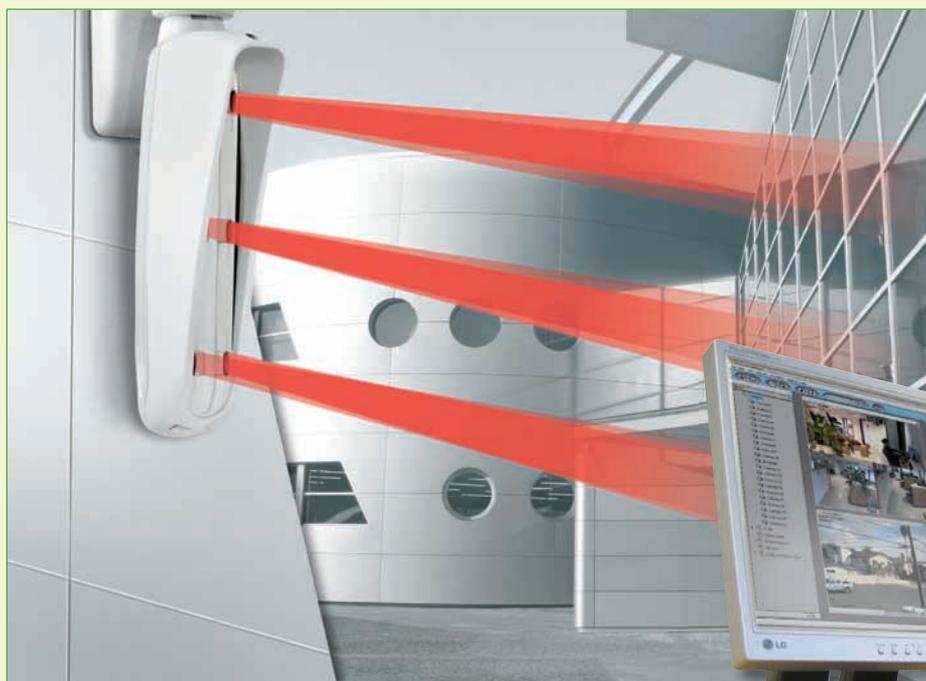
Appena entrati nel padiglione 22 che ospitava Sicurezza, ci ha accolto l'area allestita dalla Guardia di Finanza. Interessante soprattutto il simulatore ultrarealistico di una corvetta impegnata nei nostri mari: è stata riprodotta completamente la cabina di pilotaggio, la cui visuale simulata era garantita da schermi LCD uno accanto all'altro. Manovrando i comandi della plancia rispondeva un simulatore software che proiettava immagini in tempo reale di ciò che avremmo visto se fossimo veramente stati in azione, all'uscita

Il simulatore per l'addestramento militare di TESS-COM Italia.

di un porto o in alto mare, con le più svariate situazioni meteorologiche (anch'esse simulate). Giusto il tempo di farci passare il mal di mare e siamo passati a visitare gli stand di Carabinieri, Esercito, Aeronautica e tutte le altre forze dell'ordine. Ci siamo soffermati in particolare nell'area dedicata alla Polizia di Stato, dove abbiamo avuto modo di vedere veri corpi di reato (c'erano numerosi dispositivi dedicati alla duplicazione illegale di carte di credito e al furto dei dati dei Bancomat, tutti reali e tutti confiscati nel corso di operazioni) e di vedere come la Scientifica è in grado di stabilire senza possibilità di errore se un documento o una banconota siano veri o falsificati.
È incredibile quanto la tecnologia sia d'aiuto nella lotta al crimine e nella protezione del territorio: un'azienda italiana (la TESS-COM Italia S.r.l., sito Web www.tess-com.it) distribuisce in Italia un simulatore d'azione in realtà virtuale estremamente realistico, per l'addestramento di unità operative sul campo.
In pratica a un generatore di terreni 3D basato su dati reali, per nulla dissimile a un qualunque videogioco sparatutto, cuio viene aggiunta la gestione di elementi di intelligenza artificiale per la riproduzione di oggetti e persone in un ambiente plausibile (come un campo di battaglia, un quartiere cittadino sotto attacco da parte di terroristi o malviventi, uno scontro aereo o navale) con il quale i militari e forze speciali possono addestrarsi in situazioni operative quanto più vicine alla realtà.

Non mancavano aree dedicate alla Protezione Civile, alla Croce Rossa, alle Nazioni Unite e un forum sulla sicurezza personale, in particolare sulle tecniche di difesa per le donne, spesso vittime di tentativi di stupro.

:: Controllo accessi

Particolare rilevanza, su tutta l'area dei padiglioni, è stata data al controllo degli accessi ad aree private e aziendali, con o senza sorveglianza di operatori. Si tratta di sistemi che permettono di limitare in qualche modo l'accesso a determinate zone di edifici, complessi privati e industriali o aree esterne in base alle necessità del caso. I dispositivi erano numerosi e diversi: si va dalla stazione automatica per la gestione di

Questo sensore non si fa ingannare neanche da una foglia.

parcheggi pubblici e privati alla barriera a raggi infrarossi o laser che riconosce e distingue una foglia che cade dal tentativo di accesso di un veicolo o una persona non autorizzati. Ciò che emerge dal coro di proposte è la videosorveglianza, presente in fiera in tutte le salse e per tutte le tasche. In caso di stazioni di sorveglianza con operatori, la nuova tendenza strizza l'occhio all'ergonomia e alla semplicità di utilizzo (pensiamo a una stazione operativa che deve monitorare decine di videocamere di sorveglianza: umanamente impossibile senza un valido aiuto tecnologico), tanto da produrre strumenti sofisticatissimi ma anche di stile, come il Video Management Centre Eagle di Dallmeier, ideato studiando accuratamente i movimenti compiuti dagli operatori di una reale stazione di controllo e quindi razionalizzandone i comandi per offrire la massima comodità, il tutto in un oggetto di ricercato design.

Nel caso di stazioni di controllo non presidiate, tutto il carico di lavoro grava sulle macchine. Ma come fare a riconoscere potenziali situazioni di pericolo o di intrusione senza vederle direttamente? Chiaramente, la tecnologia è molto più avanti di quello che normalmente crediamo. I software di oggi sono talmente evoluti da essere in grado non solo di ricordare cose già successe, ma anche di paragonarle alla situazione attuale e stabilire quindi un livello di pericolosità in grado di far scattare un allarme, il tutto in maniera automatica. Abbiamo quindi videocamere intelligenti che vedono perfettamente anche nel buio più totale, avanzati software OCR che leggono i numeri di targa dei veicoli e algoritmi in grado di riconoscere non solo i volti delle persone ma anche i comportamenti e di prevedere lo sviluppo delle situazioni.

:: E in casa nostra?

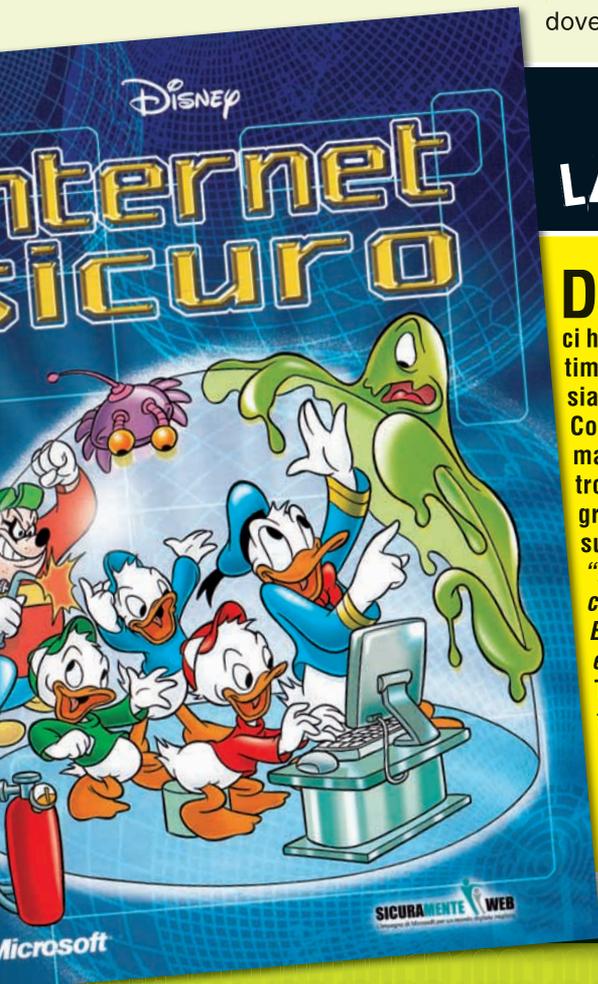
Domotica! In verità se ne fa sempre un gran parlare, ma sono ancora poche le applicazioni veramente pratiche dell'automazione domestica. Abbiamo incontrato numerose aziende che offrono i più disparati sistemi antifurto e antintrusione, da quelli più tradizionali, composti da centraline analogiche con contatti magnetici a quelli più avanzati che prevedono l'implementazione di diverse aree all'interno dello stesso appartamento. Questi ultimi si possono comandare da remoto o ci avvisano via telefono quando succede qualcosa di rilevante nella nostra proprietà; in pratica però niente di nuovo sotto il sole.

Tra tutte le aziende che hanno esposto le proprie soluzioni, Easydom (www.easydom.it) è stata una delle prime in Italia a offrire sul mercato una soluzione integrata per il controllo e la sicurezza della casa. Il sistema proposto può essere comandato da display touchscreen fissi o portatili, ma anche dal televisore di casa, su cui è in grado di funzionare anche come media center per l'intrattenimento. È completamente personalizzabile e programmabile secondo le nostre necessità e aiuta non solo a rendere la casa più vivibile e sicura, ma anche a risparmiare sulle spese energetiche, un fattore che al giorno d'oggi incide moltissimo sul bilancio di tutte le famiglie. E poi, diciamocelo chiaro, accendere l'aria condizionata con il telecomando del televisore fa figo!

Il pacchetto Technolife proposto da Alarmsystems S.r.l. invece va oltre e offre (eccolo finalmente) un sistema di domotica al passo coi tempi con l'aggiunta di una particolarità "stilosa": possiamo controllare tutto anche con l'iPod Touch o con l'iPhone (o un altro smart-phone su cui si possa installare il software necessario), usandoli come telecomandi universali per i dispositivi di casa nostra.

:: E ora parliamo di privacy

Tutto quello che abbiamo visto ci ha portato a fare alcune considerazioni di carattere generale. Innanzitutto, rimane di fondo la sensazione che la tecnologia è sostanzialmente per chi se la può permettere: non abbiamo visto strumenti veramente pronti all'uso del grande pubblico, sia come caratteristiche sia come costo. Una casa completamente automatizzata in cui un computer ci diffonde musica diversa in ogni stanza e abbassa da solo le luci per farci rilassare su un sofà da qualche migliaio di euro è sì molto bella e invitante, ma, diciamoci la verità, fa più villa "granosa" che non appartamentino da studente.

Inoltre, ci siamo chiesti più volte dove sia finita la privacy di ognuno di noi.
È bello sapere che la realtà in cui viviamo è sempre tenuta sotto controllo da qualcuno, ma davvero ci fa piacere sapere che anche lo sportello Bancomat è in grado di riconoscerci, e non solo perché abbiamo inserito la nostra tessera per prelevare?
Siamo quasi ai limiti del sopportabile, dove in presenza di una supervideocamera intelligente e automatica che vede anche al buio o nella nebbia, rischiamo di essere fermati per un controllo dopo aver dato una manata sulla spalla di una nostra amica per scacciare un piccolo insetto. E solo perché quel gesto viene interpretato da queste moderne tecnologie come un'aggressione in corso. Come sempre, il tutto sta nell'uso che ne facciamo: avere la possibilità di fare qualcosa non vuol dire per forza che la si debba fare...

Sicurezza sul Web: la parola al poliziotto

Durante la nostra visita allo stand della Polizia di Stato abbiamo avuto modo di scambiare due parole con un rappresentante del corpo, molto disponibile, che ci ha dato interessanti informazioni su quali sono le principali aree su cui il dipartimento di Polizia Postale e delle Comunicazioni opera normalmente e su quali siano le minacce alla sicurezza cui fa fronte quotidianamente.
Con nostra sorpresa, forse perché è al centro del nostro lavoro, la frode informatica compiuta sul Web non è la prima delle preoccupazioni degli agenti: purtroppo in testa a questa triste classifica troneggia il reato a sfondo pedopornografico, cioè l'adescamento di minori e lo scambio di materiale multimediale sull'argomento. *"Benché più diffusi e numerosi"*, ci ha spiegato il funzionario, *"i reati come la truffa su eBay, il phishing o lo scambio illegale di materiale coperto da diritti d'autore sono meno gravi di quelli che coinvolgono i bambini. Ecco perché diamo precedenza a questi ultimi e investiamo molto in tecnologie e persone per far fronte a questo problema"*. Come dargli torto?
Tra i mezzi di prevenzione proposti dalla Polizia Postale ce n'è uno rivolto direttamente ai più piccoli: un fascicoletto nato dalla collaborazione tra Walt Disney italia e Microsoft che, con l'aiuto dei paperi più famosi del mondo, spiega quali siano i pericoli che si possono incontrare sul Web e come difendersi.
Lo possiamo scaricare all'indirizzo http://www.poliziadistato.it/pds/informatica/index.htm facendo clic su Internet sicuro.

Sinowal l'immortale

La minaccia russa continua a mietere vittime

Si prenda un trojan, gli si dia la capacità di rubare dati personali a un utente, e lo si maschieri per bene dalle scansioni degli antivirus: la ricetta del crimine informatico perfetto sta tutta qui. Peccato, anzi per fortuna, che ben pochi truffatori digitali siano riusciti in questa sordida impresa. O per lo meno, chi ci è riuscito non ha mai potuto cantare vittoria per lungo tempo. Questo fino a oggi, perché il temibile Sinowal, trojan anche conosciuto come Torpig e Mebroot, in realtà miete tuttora le sue vittime.

Molte, moltissime vittime: in circa due anni, infatti, ha rubato oltre 300.000 dati d'accesso a servizi bancari, e più di 300.000 numeri di carte di credito. Insomma, per longevità e quantità, un record che, sebbene abbia attirato l'attenzione dei maggiori esperti di sicurezza informatica, è in grado di migliorarsi giorno dopo giorno. Il segreto di questo poco apprezzabile successo non sta in qualche fantomatica tecnica di replicazione del codice malevolo, ma in un costante aggiornamento da parte dei suoi autori. Ma andiamo con ordine: Sinowal è a tutti gli effetti un trojan, quindi di un programma di modeste dimensioni privo della capacità di replicarsi, in grado di mettere in contatto il computer della vittima col truffatore. Quest'ultimo, poi, assume il controllo di alcune funzioni vitali del computer. Dunque, come ogni trojan che si rispetti, Sinowal basa la sua vita su tre distinte fasi: la sua installazione nel computer-vittima, il suo mascheramento e, infine, l'attivazione di un sistema di comunicazione col truffatore.

Sinowal finora ha colpito oltre 500.000 account e servizi web personali.

:: Una "injection" dolorosa

Nel caso di Sinowal, la prima fase consiste in una normale procedura di HTML injection. In pratica il codice malevolo su cui si basa, è collegato a qualche contenuto web (di solito dei Java script) che viene integrato in una qualsiasi pagina di un sito Internet.

Quando l'utente visualizza la pagina, e quindi di fatto la carica in memoria, il codice ha modo di installarsi nel suo computer. Non è questo il contesto per scendere nei dettagli di questa tecnica, ma ci basti sapere che, sebbene vecchia come il cucco, è tuttora molto efficace e per questo una delle più diffuse in quanto, come sappiamo, è piuttosto semplice far credere a un browser che sta caricando dei contenuti assolutamente innocui.

```
0000:  FA 33 DB 8E D3 36 89 26 FE 7B BC FE 7B 1E 66 60  .3...6.&.{..{.f`
0010:  FC 8E DB BE 13 04 83 2C 02 AD C1 E0 06 8E C0 BE  .......,........
0020:  00 7C 33 FF B9 00 01 F3 A5 B8 02 02 B1 3D BA 80  .|3..........=..
0030:  00 8B DF CD 13 33 DB 66 8B 47 4C 66 26 A3 73 00  .....3.f.GLf&.s.
0040:  C7 47 4C 66 00 8C 47 4E 06 68 4D 00 CB FB 8E C3  .GLf..GN.hM.....
0050:  B8 01 02 B9 3F 00 BA 80 00 B7 7C CD 13 66 61 1F  ....?.....|..fa.
0060:  5C EA 00 7C 00 00 9C 80 FC 42 74 0B 80 FC 02 74  \..|.....Bt....t
0070:  06 9D EA 00 00 00 00 2E 88 26 90 00 9D 9C 2E FF  .........&......
0080:  1E 73 00 0F 82 9D 00 9C FA 06 66 60 FC B4 00 B5  .s........f`....
0090:  00 80 FD 42 75 04 AD AD C4 1C 85 C0 75 01 40 8B  ...Bu.......u.@.
00A0:  CB B0 8B C1 E1 09 8B FB 60 F2 AE 75 47 66 26 81  ........`..uGf&.
00B0:  3D F0 85 F6 74 75 F2 26 81 7D 05 80 3D 75 EA 26  =...tu.&.}..=u.&
00C0:  8A 45 04 3C 21 74 04 3C 22 75 DE BE 0B 02 2E 80  .E.<!t.<"u......
00D0:  3C 00 75 20 2E 88 04 26 C7 45 FF FF 15 66 8C C8  <.u ...&.E...f..
00E0:  66 C1 E0 04 05 00 02 66 2E A3 FC 01 2D 04 00 66  f......f....-..f
00F0:  26 89 45 01 61 B0 83 F2 AE 75 25 66 26 81 3D C4  &.E.a....u%f&.=.
0100:  02 E9 00 75 F2 66 26 81 7D 04 00 E9 FD FF 75 E7  ...u.f&.}.....u.
0110:  66 26 C7 45 FC 90 90 90 83 26 83 65 06 00 EB D7  f&.E.....&.e....
0120:  66 61 07 9D CA 02 00 00 00 00 00 00 00 00 00 00  fa..............
0130:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0140:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Un esempio di codice MBR alterato da codice malevolo.

A questo punto, un normale trojan si limiterebbe a risiedere nella memoria locale del computer, ma è qui che Sinowal dà il meglio di sé, andando a installarsi invece nel MBR. Il Master Boot Record è un piccolo programma che viene caricato durante l'avvio di un computer, e risiede di solito nel primo settore del disco fisso. Scopo del MBR è di controllare in un'apposita tabella quale partizione va caricata e passare il controllo al settore di boot di questa. Capiamo bene che la presenza di codice malevolo in questa zona di memoria è tra le più "privilegiate" e Sinowal non è l'unico ad approfittarne. Tuttavia, a differenza di altre minacce informatiche, questo trojan non modifica in alcun modo l'MBR e gli antivirus, per questo motivo, non sono in grado di rilevarlo. Sinowal attende che il PC sia avviato una prima volta, entra in azione dopo otto minuti (evitando la scansione iniziale operata da molti antivirus), modifica il registro di Windows e, quindi, riavvia il computer sfruttando una copia alterata del MBR. Al contempo, il trojan elimina tutte le sue tracce.

:: Registratore malevolo

Una volta installato e attivato, Sinowal entra in azione. E qui, dopo la tecnica del MBR vista poco fa, rivela il suo secondo asso nella manica.

Perché non ci diamo un'occhiata da vicino? Di fatto, lo scopo primario di questo trojan è di fungere da "keylogger", quindi registrare le stringe digitate dall'utente sulla tastiera. Tuttavia, dato che in poche ore un utente può digitare decine di migliaia di caratteri, il truffatore rischia di ritrovarsi con enormi file di testo da setacciare, alla ricerca di password e account per accedere ai più disparati servizi online. Sinowal invece si rifà a un archivio di indirizzi web che lo attivano al momento giusto. Quindi se per esempio la vittima digita l'indirizzo del servizio di banking online che è solita utilizzare, e questo è tra quelli considerati dall'archivio di Sinowal, il trojan si attiva registrando i dati di accesso e inviandoli al truffatore. Ciò, ovviamente, richiede il collegamento a Internet, ma è pur vero che per accedere a dei servizi web la vittima deve per forza essere online, quindi...

Anche la versione gratuita di Avira Antivir è in grado di combattere Sinowal.

:: Questione d'aggiornamento

La potenza di Sinowal deriva in buona parte anche dall'aggiornamento maniacale del suo archivio, perpetrato dagli autori. Una vera e propria gang criminale, probabilmente russa, che ha già raccolto e "verificato" circa 3.000 siti Web.
E, zelante com'è, apporta continui miglioramenti al codice malevolo del trojan stesso, modificandolo quel tanto che basta a mettere KO quei pochi antivirus in grado di riconoscerlo. Al che, sorge spontanea la domanda: "cosa si può fare per combattere Sinowal e le sue varianti"? Innanzitutto, va sottolineato che il trojan colpisce primariamente Windows XP. Anche le versioni più aggiornate, che pur limitando gli accessi al MBR, non possono bloccare quelli ad alcuni settori iniziali del disco fisso. A conferma che, per quanto abbia i suoi problemi, Windows Vista è piuttosto efficiente sul profilo della sicurezza, arriva la notizia che il più recente sistema operativo di Microsoft è immune, al momento, alla minaccia. E per chi preferisce ancora XP? Mentre Sinowal ha messo, e continua a mettere, in ginocchio i più blasonati antivirus, pare che Avira (www.free-av.com), freeware, lo riconosca senza problemi. O almeno, sia in grado di farlo fino ad oggi. Del doman, specie se si ha a che fare con Sinowal, non v'è certezza.

I miti e le statistiche che infiammano la guerra dei browser

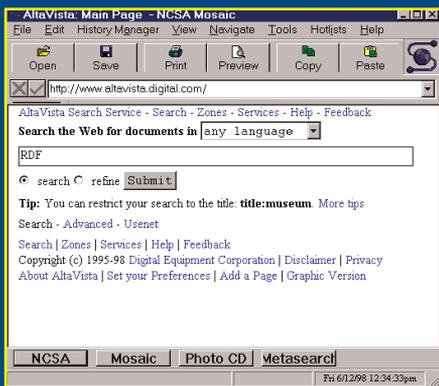
TUTTO È RELATIVO

Quando, una quindicina d'anni fa, il Web ha iniziato timidamente a fare capolino nelle nostre case non c'erano molte scelte. I pochi super appassionati che volevano disporre di una connessione a Internet ottenevano dal proprio provider un kit per la fruizione dei servizi contenente il browser disponibile al tempo, sostanzialmente NCSA Mosaic che possiamo definire tranquillamente l'antesignano di quasi tutti i browser Web attuali. Ma, come ben sappiamo, lo sviluppo di Internet fu importante e repentino e la situazione cambiò rapidamente.

:: Microsoft Vs. Netscape

Nel 1994 Marc Andreessen, leader del team che stava dietro al progetto Mosaic, fondò la propria azienda, la Netscape Communications Corporation. Lanciò e promosse quindi quello che sarebbe in breve diventato il browser più usato sul Web: Netscape Navigator. Disponibile gratuitamente per organizzazioni senza scopo di lucro e per enti educativi, e in versione trial per il resto degli utenti (ma senza alcuna limitazione, il che lo rese de facto gratuito per tutto il pubblico), Netscape Navigator conquistò nel giro di un paio d'anni ben l'80% del mercato dei tempi, anche perché al di fuori degli ambienti accademici non esistevano concorrenti.

Bill Gates inizialmente snobbò il mercato del Web, definendolo come una moda passeggera che presto sarebbe rientrata in ambito accademico. Non il primo dei grandi errori commessi da zio Bill, per cui "640 KB di memoria sono sufficienti per tutti"...

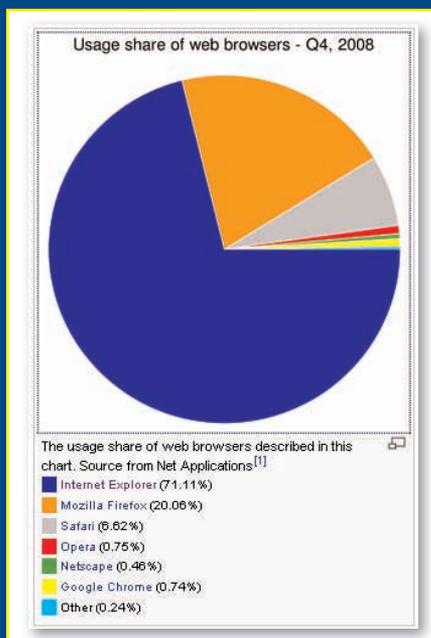
Ma l'animo commerciale di Microsoft non si fece attendere oltre. Acquistati i diritti di sviluppo di Internet Explorer da Spyglass Inc. si mise in diretta concorrenza con Netscape, sfruttando la situazione predominante di produttore del sistema operativo più usato al mondo e integrandovi strettamente il proprio browser, fatto che causò non pochi grattacapi legali alla casa di Redmont. La "Guerra dei browser" era iniziata.

La schermata di NCSA Mosaic, il primo browser Web a larga diffusione.

:: Terreno fertile

Da allora di browser per il Web ne sono nati e morti moltissimi. In alcuni casi si trattava di banali implementazioni di motori Web esistenti con l'aggiunta di alcuni fronzoli, in altri di veri e propri browser a parte. Da quando, verso il 2000, si è consolidata la differenziazione tra motore di rendering delle pagine Web e interfaccia utente, chiunque può scriversi il proprio browser pescando dal primo e aggiungendo elementi per la seconda. Tuttavia, proprio per la posizione predominante già citata, a Microsoft non costò nulla raggiungere in breve tempo il 95% del mercato, mentre Navigator, un po' lasciato in balia delle correnti, ha visto sempre più diminuire i propri utenti, fino a morire poco gloriosamente nel 2007, quando AOL (attuale detentrice dei diritti) cessò di fornire supporto al browser che ha avvicinato moltissimi utenti al mondo del Web.
Negli ultimi anni, Microsoft ha perso per legge (ma non di fatto) la sua posizione predominante, e l'utente di oggi ha ampia scelta a disposizione per provare e selezionare il programma che più incontra le proprie preferenze. Ci avviciniamo alla Guerra dei browser atto secondo.

:: Tutto è relativo

Da quando il Web è diventato un mezzo popolare di comunicazione e di divulgazione delle informazioni, le statistiche di utilizzo di un determinato browser sono sotto gli occhi di tutti. Basta però visitare due o tre siti diversi per rendersi conto di come i dati presentati siano tutto fuorché congrui. Secondo autorevoli fonti, Internet Explorer darebbe a Microsoft ancora la supremazia con un buon 71% del mercato attuale. A un browser emergente quanto apprezzato come Firefox spetterebbe un 20% abbondante, mentre tutti gli altri browser si dividerebbero con fortune alterne il restante 9% del mercato.
Questi dati li troviamo per esempio in Wikipedia, che offre una pagina aggiornata al mese precedente e che si può raggiungere all'indirizzo **http://en.wikipedia.org/wiki/Usage_share_of_web_browsers**. Ma siamo certi che questi dati corrispondano al vero?

L'adagio di Einstein si adatta bene anche a questo argomento. Se per esempio andiamo a consultare le statistiche divulgate da W3Schools.com (un popolare sito che offre un buon punto di partenza per chi vuole imparare a programmare per il Web), notiamo invece che Internet Explorer si attesta intorno al 47%, Firefox al 44% e Safari, Opera, Mozilla e Chrome (quest'ultimo con una buona impennata dal momento del rilascio) si spartiscono il rimanente 9%. Ben lontano dai numeri precedenti.

I dati sulla diffusione dei browser attuali, registrati sul sito di Wikipedia.

Netscape Navigator 2.0, i supporti di installazione. Grazie a questo browser oggi abbiamo Javascript e i Preferiti o Segnalibri.

:: Come è possibile?

Sono diversi i fattori che influenzano questi risultati. Per prima cosa, teniamo presente che la maggior parte degli accessi registrati non avviene da parte degli utenti, bensì dei bot dei motori di ricerca che arbitrariamente possono indicare come user agent (ovvero l'identificazione del browser usato) uno qualunque dei browser disponibili. In secondo luogo, il browser rilevato dipende in gran parte dall'area tematica del sito. Un sito che parla di sviluppo Web è più visitato da chi fa uso di browser alternativi a Explorer, Firefox in testa. Uno di cucina probabilmente è visitato da chi usa il browser predefinito del sistema operativo, nella maggior parte dei casi Internet Explorer. Non solo: le statistiche vengono spesso falsate e risultano diverse in base al tempo in cui vengono consultate. Immediatamente dopo il lancio di un nuovo browser o di una nuova release di uno già esistente, si ha sempre un'impennata di quel determinato browser. Esiste solo un modo quindi per produrre pagine Web che vengano visualizzate correttamente da tutti: basarsi solo sullo standard W3C, e ignorare le peculiarità dei singoli browser. Fino a quando non saranno tutti d'accordo.

PIÙ TORRENT PER TUTTI

Come scaricare alla massima velocità e in sicurezza

Chi di noi non ha scaricato qualcosa via peer to peer e ha sbattuto la testa con le povere derelitte linee italiane? Altro che ore... giorni per completare un download un po' "importante". Inoltre, specialmente nel caso di chi preferisce avere a che fare con i torrent, non è facile trovare un tracker affidabile, dato che la maggior parte dei migliori sono privati che non consentono facilmente l'accesso.
Le soluzioni sono due: o ci armiamo di santa pazienza e aspettiamo il tempo dovuto prima di avere il file sul nostro disco, o ci affidiamo a una seedbox. In questo caso, però, si tratta di un servizio a pagamento.

:: Download continuo

La differenza tra l'uso di un normale PC collegato a Internet e l'uso di una seedbox consiste nel luogo in cui risiede il software che si occupa del download dei torrent. Mentre nel nostro PC di casa avremo un programma come BitTorrent o Vuze, che si usa come un normale software P2P, lasciando il PC collegato interminabili ore (impossibile con una tariffa a consumo) e in balia dei capricci della connessione, usando una seedbox avremo un server online assolutamente privato che si occuperà di scaricare i file al nostro posto. Sfruttando semplicemente la propria natura di server (connessione super veloce sia in download sia in upload) e la facilità di gestione dei file via browser. Ma, come abbiamo detto, si tratta di un servizio a pagamento, chi mai e poi mai sarebbe disposto a pagare per scaricare file, giri pagina e passi all'articolo seguente. Tuttavia i costi non sono eccessivi, e volendo si può sacrificare una pizza al mese per pagarsi una seedbox che scarichi film e musica per noi, senza intasare il nostro PC di programmi famelici di risorse.

:: Come funziona

Il principio non è molto dissimile da un normale servizio di hosting sul Web, come quello offerto da molti provider. Una volta sottoscritto l'abbonamento,

abbiamo a disposizione una macchina su Internet che, invece di offrire servizio Web ai visitatori dei nostri siti, si occuperà di far girare il programma adatto per scambiare torrent con altri utenti (anche se questi non hanno a loro volta una seedbox). Questo nostro server privato sfrutterà tutta la banda a sua disposizione che normalmente è molto più ampia di quello che il nostro provider ci concede. Di conseguenza, il download di un file molto pesante impiegherà meno tempo per essere completato.
Nel frattempo noi possiamo controllarne l'avanzamento tramite una comoda interfaccia Web. Quando il trasferimento è terminato e il file è completo e disponibile, possiamo semplicemente scaricarlo sul nostro computer come se fosse un normale download via browser, quindi molto più velocemente di qualsiasi trasferimento P2P.

:: Quanti vantaggi!

La velocità non è l'unico vantaggio che ci offre una seedbox. Uno dei plus aggiuntivi risiede nel fatto che non dobbiamo tenere numerosi file incompleti sparsi sul nostro PC, lasciando spazio libero per altre applicazioni. Quando un download è terminato, sia esso di un file multimediale piuttosto che di un programma, dobbiamo semplicemente scaricarlo dalla seedbox e scegliere se avviarlo (e cancellarlo dopo l'uso) o masterizzarlo su cd/dvd: rimarrà comunque una copia sul server per quando ci servirà ancora, o fino a quando decidiamo di lasciarvelo.
Con questo sistema, anche chi dispone di un abbonamento a Internet "a consumo" potrà godersi un po' di sano P2P: la banda usata realmente per lo scarico non ha nulla a che vedere con quella che ci concede il nostro provider e quindi scaricare via seedbox non intaccherà la nostra quota. O meglio, lo farà solamente quando decideremo di prelevare il file, utilizzando solo il traffico strettamente necessario. Un altro vantaggio non indifferente è legato al problema dei tracker. Come sappiamo, quest'ultimi sono privati e molto schizzinosi, accettano con un buon rank solo chi ha molti file, molta banda e molta presenza online. Da casa è raro (e comunque pericoloso) raggiungere tali risultati, ma con una seedbox sempre online e al massimo della velocità le cose cambiano, e anche noi potremo entrare nell'elite della condivisione sul Web.
Infine, per chi ama la privacy, va ricordato che per sua natura questo sistema mette al riparo da ogni tracciamento, sul proprio PC non rimane alcun segno dell'attività di condivisione e tutti i file sono in un server sicuro e lontano da casa.

Alcune soluzioni per attivare subito la nostra seedbox.

:: Dove le troviamo?

Non sono molti i provider che offrono servizio seedbox, e comunque sono loro che si sobbarcano tutti gli oneri della condivisione, quindi non è detto che chi troviamo oggi sia ancora in linea domani con tale servizio.
Tra quelli che offrono l'interfaccia più comune, chiamata TorrentFlux, troviamo per esempio We Will Host It (http://wewillhostit.com/), che ci mette a disposizione una seedbox a partire da 8 dollari al mese. Per questa cifra avremo a disposizione 5 GB di spazio. W00ts!te Solutions (http://www.w00tsite.com/ e http://www.seedm8.com/) offre invece 4 GB, due torrent in trasferimento a 100 KB/secondo per 5 dollari al mese. LeaseTorrent.com (http://www.leasetorrent.com/) offre download fino a 100 Mbps, 10 GB di spazio e traffico limite di 200 GB al costo di 15 dollari al mese. Infine, tra i più costosi, Seedbox Hosting (http://seedboxhosting.com/seedbox/).
Per la "modica" cifra di 47 dollari al mese avremo a disposizione (ma non in tempi brevissimi) una macchina dedicata con 50 GB di spazio su disco, 250 MB di RAM e trasferimenti illimitati. Per pochi fortunati.

Le cartelle fantasma

In molte versioni di Windows esistono cartelle condivise sospette. Scopriamole

Attivando il servizio Condivisione file e stampanti di Windows appaiono delle cartelle condivise nascoste che non è possibile gestire direttamente. Che scopo hanno? Innanzitutto, vediamo di quali cartelle si tratta. Per controllare quali siano le risorse in condivisione la via più semplice è fare clic su Start/Impostazioni/Pannello di controllo/Strumenti di Amministrazione/Gestione Computer. Poi su Cartelle condivise/Condivisioni. Quelle che troviamo in elenco sono tutte le condivisioni del computer, incluse quelle nascoste. La cosa sorprendente è che anche se non abbiamo condiviso alcuna cartella sul nostro PC, troveremo una serie di condivisioni il cui nome termina con il simbolo del dollaro e che corrispondono alle lettere dei dischi installati. Inoltre esisteranno almeno altre due condivisioni, ADMIN$ e IPC$.

:: Le condivisioni predefinite

Altrimenti chiamate Default Shares, si tratta di condivisioni di sistema create da Windows per la gestione interna dei dischi e di altre caratteristiche del sistema operativo. Non sono quindi cartelle vere e proprie, ma semplicemente condivisioni che si riferiscono a determinati elementi a cui il sistema deve accedere per permettere operazioni particolari o per la gestione dell'ambiente di rete. Solo per comodità ci si riferisce a queste condivisioni con il termine "cartelle", e in alcuni casi è anche vero, ma in realtà si tratta di astrazioni: la cartella condivisa nascosta PRINT$ è creata dal sistema per la gestione delle stampanti di rete e non si tratta quindi di una cartella reale ma, diciamo così, indica la strada ai computer della rete per raggiungere una stam-

pante condivisa, mappandola come se lo fosse. Lo stesso accade se troviamo sul nostro computer la cartella FAX$.

Un caso diverso riguarda ADMIN$ e IPC$. La prima si riferisce alla cartella principale di Windows sul nostro sistema, normalmente C:\Windows o C:\WinNT. La seconda mappa su una cartella virtuale la comunicazione tra client e server per la gestione da remoto dei server di rete. Le rimanenti cartelle che possiamo trovare, questo dipende dal nostro PC, sono C$, D$ e così via per tutte le lettere di unità disco presenti nel sistema.

A questo punto possiamo intuire da soli quali possono essere i pericoli di queste condivisioni: chiunque riuscisse ad avere accesso da remoto al nostro PC, avrà in mano il nostro sistema. Nel vero senso della parola, potrà operare come se fosse fisicamente alla tastiera, eliminando o spostando file e compromettendo il funzionamento del PC.

Le condivisioni predefinite che si trovano su un PC con Windows XP.

:: Facciamo una prova

Se abbiamo modo di collegare in rete due computer, possiamo fare una prova e imparare sul campo quanto possano essere pericolose le condivisioni predefinite di Windows.

Il primo computer è quello che usiamo come "vittima" e lo chiamiamo "Orco". Il secondo è quello da cui agiamo e lo chiamiamo "Elfo". Sul computer Orco installiamo Windows XP Professional con le impostazioni di base, assicurandoci di aver correttamente configurato la rete. Meglio se usiamo un indirizzo IP fisso, per esempio 192.168.1.101 per Elfo e 192.168.1.102 per Orco, e assicuriamoci anche che i due PC facciano parte dello stesso gruppo di lavoro (WORKGROUP è quello predefinito di Windows e va benissimo per il nostro scopo). Quando tutto è a posto verifichiamo che i due PC possano comunicare via rete: apriamo una finestra del DOS (Start/Tutti i programmi/Accessori/Prompt dei comandi) e scriviamo da Elfo "ping 192.168.1.102". Se non otteniamo errori di richiesta scaduta, i due computer sono in rete e possono comunicare tra loro.

Ora tentiamo di accedere a Orco lavorando su Elfo. Possiamo farlo direttamente da Risorse del computer: se scriviamo nella barra dell'indirizzo \\Orco\C$, dovremmo poter accedere a quella condivisione senza problemi e vedere il contenuto del disco C. Niente: una bella finestra di errore ci avvisa che non è possibile raggiungere il computer desiderato. Questo perché ancora Orco non condivide niente: il servizio di rete non è pronto per accettare connessioni dall'esterno.

Proviamo quindi a creare una condivisione standard su Orco: prepariamo una nuova cartella nel disco C e la chiamiamo Rete, facciamo clic destro sulla sua icona e scegliamo Condivisione e protezione dal menu di scelta rapida e attiviamo la condivisione in rete della cartella, con lo stesso nome. Per verificare che in effetti quello che vedremo su Elfo è quello che Orco condivide, copiamo un file qualsiasi nella cartella Rete. A questo punto, se tentiamo di accedere alla cartella condivisa con \\Orco\Rete dovremmo vedere il file copiato in precedenza, quindi tutto regolare. Ora facciamo di nuovo la prova con la condivisione predefinita e scriviamo \\Orco\C$. Le cose sono cambiate: molto probabilmente troveremo una bella fine-

Tentativo di accesso, senza successo, al PC Orco che ancora non condivide niente.

strella che ci chiede nome utente e password per accedere alle risorse condivise da Orco. Ma, se osserviamo bene, il nome utente è forzato come Guest, e non è possibile modificarlo. A questo punto è chiara una cosa: se conosciamo la password dell'utente Guest di Orco possiamo accedere alle risorse condivise da quest'ultimo, ma non avremo alcun privilegio particolare. Si tratta di una precauzione presa da Microsoft nelle ultime versioni di Windows denominata "ForceGuest" e serve per evitare che un utente remoto riesca ad accedere con privilegi da amministratore ai dischi di un computer in rete. Fin qui, quindi, tutto bene.

:: Ma se il PC è datato?

Chi smanetta un po' con hardware e software ha spesso in casa uno o più PC vetusti, che tiene in vita per il gusto di vederli funzionare.

Gli si danno i compiti più disparati: player MP3, router o firewall per la rete, computer per giocare a vecchi videogames e chi più ne ha...

Su questi computer spesso non si riesce a installare le ultime versioni di Windows, vuoi perché sono troppo

e tentiamo di accedere a una condivisione predefinita di XP, vedremo questa finestra.

vecchi e poco potenti per poter far girare XP o Vista, vuoi perché un componente hardware che ci è indispensabile per lo scopo cui abbiamo tenuto in vita quel PC non è più supportato dai nuovi sistemi operativi. Si finisce quindi a ripiegare a vecchie versioni di Windows, come NT4 o 2000, quest'ultimo ancora gloriosamente in auge grazie all'incredibile (per quei tempi) stabilità. Abbiamo quindi un bel Pentium III a 800 MHz con Windows 2000 Professional e un disco da 80 GB che magari ci fa da server di stampa e da file server per la rete di casa. Ottimo. Molto probabilmente, quel PC sarà perennemente acceso, per essere sempre disponibile a tutta la famiglia nel momento del bisogno.
Questo significa che sarà perennemente disponibile anche a chi, dall'esterno, è in grado di penetrare attraverso le nostre "difese". Basta sapere infatti l'IP pubblico con cui accediamo a Internet e con un network scanner si può avere una chiara idea di come sia composta la nostra rete locale.
Nmap è in grado anche di dire quale sistema operativo è installato su ciascuna macchina: dire all'esterno che sul nostro computer gira Windows 2000 vuol dire "prego, accomodati"! Se infatti proviamo lo stesso giochetto con Windows 2000 e tentiamo di accedere con l'utente Administrator, possiamo tranquillamente compiere tutti i tentativi che vogliamo per indovinare la password di accesso. Spesso quest'ultima è inesistente, oppure è talmente banale che con un attacco via dizionario avremo porte spalancate sulle condivisioni di sistema, quindi al disco C del computer.
Eliminiamo un file qui e un file lì, oppure copiamo un file maligno nella cartella Esecuzione automatica, e al prossimo riavvio quel PC sarà infetto e in nostro controllo...

La chiave di registro da creare o da modificare per disabilitare le condivisioni predefinite.

:: Come difenderci

Purtroppo non esiste un metodo definitivo per evitare che il sistema crei queste condivisioni predefinite.
Si tratta infatti di elementi vitali per il funzionamento dei servizi di rete, pertanto, per essere certi di stare al sicuro, dovremmo evitare di mettere in rete un computer potenzialmente pericoloso.
La regola numero uno, comunque, è una corretta implementazione delle password del sistema. Soprattutto per quanto riguarda l'account Administrator. Meglio una password composta da caratteri diversi e apparentemente senza senso, comprendente lettere, numeri e simboli, magari più

difficile da ricordare ma sicuramente anche più difficile da individuare da parte di un malintenzionato. Per esempio, possiamo usare lo "slang scritto" che spesso si trova in uso nei siti hacking che sostituisce numeri e simboli ad alcune lettere: la password "letmein" in slang può diventare "l3tm3!n", abbastanza complessa per un tentativo di brute forcing.
Se vogliamo essere certi che, appena avviata la macchina, queste condivisioni non siano accessibili dall'esterno, possiamo eliminarle manualmente. In questo caso però la cosa è fattibile solo su un PC che non ha bisogno di condividere cartelle. Possiamo agire in due modi. Apriamo il Pannello di controllo, facciamo doppio clic su Strumenti di amministrazione e poi su Gestione computer. Apriamo quindi Cartelle condivise e facciamo clic con il pulsante destro sulla condivisione da eliminare, quindi scegliamo Termina condivisione e confermiamo con OK. Il computer ci avviserà che, trattandosi di una condivisione predefinita, verrà ricreata al prossimo avvio del sistema.
Il secondo metodo, per gli smanettoni del DOS, consiste nell'aprire una finestra del Prompt dei comandi e inserire, una dopo l'altra, le seguenti linee:

```
Net Share C$ /delete
Net Share D$ /delete
Net Share E$ /delete
Net Share F$ /delete
Net Share ADMIN$ /delete
```

Naturalmente in base ai dischi installati sul vostro sistema: se non avete il disco F, è inutile tentare di eliminare la condivisione F$.
Se vogliamo liberarci definitivamente da queste condivisioni (ma ricordiamoci, a questo punto non potremo più condividere risorse in rete) possiamo cambiare una chiave del registro con regedit (se non troviamo questa chiave, possiamo crearla noi).

Nei sistemi operativi Server (Windows NT 4.0 Server, Windows 2000 Server e Windows Server 2003):

Gruppo: HKEY_LOCAL_MACHINE
Chiave: SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
Nome: AutoShareServer
Data Type: REG_DWORD
Valore: 0
Nei sistemi operativi workstation (Windows NT 4.0, Windows 2000 Professional, Windows XP):
Gruppo: HKEY_LOCAL_MACHINE
Chiave: SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
Nome: AutoShareWks
Data Type: REG_DWORD
Valore: 0

:: Un trucchetto

Il simbolo del dollaro in fondo al nome di queste condivisioni indica che si tratta di condivisioni nascoste: non sono visibili all'utente normale che accede alle risorse di rete.

Sapendolo possiamo creare una condivisione nascosta per i nostri scopi: basta infatti aggiungere il simbolo del dollaro al nome che abbiamo scelto, per esempio Rete$ o Condivisa$. Naturalmente, siamo ben consci che in questo modo dovremo attivare i servizi di condivisione e quindi siamo più a rischio, vero? Non dimentichiamo quindi di dare una controllatina alle password.

OSfuscate

Cambiamo l'impronta del sistema operativo per non farlo rilevare via web

Sappiamo tutti che chiunque possa scegliere se sferrare un attacco a una macchina Windows o una Linux non ha alcun dubbio: Windows (ahimè) è per sua natura un parco giochi per i malintenzionati della Rete, che possono cambiare exploit così come cambiano il guardaroba con le nuove stagioni, certi che prima o poi il varco lo troveranno.
Questo perché, già nel momento stesso del primo sondaggio della macchina vittima, è molto facile sapere quale sistema operativo sia in funzione, è un dato deducibile con semplicità dalle caratteristiche TCP/IP riscontrate.
Se quindi vogliamo passare sonni più tranquilli mentre di notte lasciamo il PC acceso scaricando a manetta sul Mulo, è meglio confondere un po' le nostre tracce e far credere agli eventuali intrusi in ascolto che nel nostro PC sia installato un sistema operativo diverso dal reale.

È facile scoprire quale sistema operativo usiamo con un programma com Nmap, NetworkMiner oppure Ettercap.

:: Il principio

Programmi come Nmap, Ettercap o NetworkMiner sono in grado di riconoscere un sistema operativo grazie alle peculiari impostazioni TCP/IP dello stesso. Vale a dire, quando trova una particolare sequenza di impostazioni, è certo di essere in presenza di una macchina Windows, oppure Linux oppure BSD e via dicendo.
Il ragionamento alla base quindi è questo: se cambiamo il modo in cui lo stack TCP/IP della nostra macchina viene letto dall'esterno, è probabile che il programma usato per spiarci lo confonda con quello di un altro sistema o non sia in grado del tutto di

rilevarlo. La cosa però deve essere fatta con attenzione, per non provocare malfunzionamenti. Sappiamo che Windows conserva tutti i dati di configurazione nel file di registro. È quindi sul registro che, con tutte le precauzioni del caso, dobbiamo intervenire. Per prima cosa, facciamo una copia di riserva del registro stesso per poterlo ripristinare in caso di problemi. A questo scopo possiamo usare un apposito programma di utilità, come ad esempio ERUNT (lo possiamo scaricare all'indirizzo http://www.larshederer.homepage.t-online.de/erunt/). Se poi abbiamo un altro computer in rete, possiamo usarlo come macchina per i test installandovi i programmi che servono allo scopo (Nmap per esempio). Da lì faremo partire le scansioni verso il nostro PC prima e dopo aver offuscato l'impronta del sistema operativo.

:: Cosa cambiare

Abbiamo davanti a noi due strade: la prima è quella di agire manualmente; in questo caso apriamo il file di registro con Regedit (se non abbiamo creato una scorciatoia per avviarlo, possiamo farlo con Start/Esegui/regedit.exe). Le voci che dobbiamo cambiare sono tutte salvate in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** e sono le seguenti:

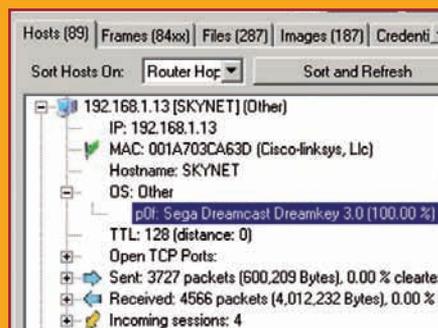
DefaultTTL
Tcp13230pts
EnablePMTUDiscovery
TcpUseRFC1122UrgentPointer
TcpWindowSize
SackOpts
Interfaces*\MTU

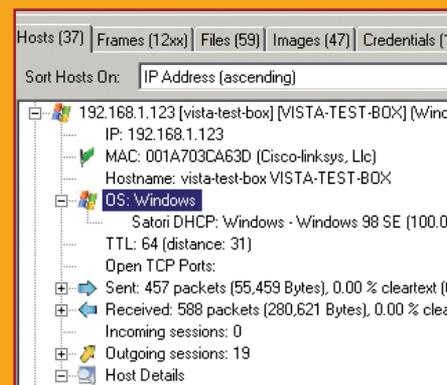
Non possiamo ovviamente inserire valori a caso, e non solo perché così rovineremmo con tutta probabilità il funzionamento del nostro sistema, ma anche perché il nostro scopo è far credere agli attaccanti di trovarsi davanti a un diverso sistema operativo. Dovremo quindi recuperare informazioni su come sono impostati questi parametri nel sistema operativo che vogliamo simulare. Una buona fonte di informazioni a questo proposito è la guida di Nmap, che possiamo trovare all'indirizzo http://nmap.org/book/toc.html. In particolare, il capitolo 8 è completamente dedicato all'individuazione del sistema operativo.
La seconda strada è quella di affidarsi a un programma capace di svolgere direttamente tutte queste operazioni.

L'interfaccia di inserimento di OSfuscate ti fa scegliere chi vuoi essere.

OSfuscate è un software espressamente progettato per questo, dobbiamo solo lanciarlo, scegliere quale sistema operativo vogliamo imitare e permettergli di cambiare il registro di Windows in autonomia. Lo possiamo scaricare dall'indirizzo http://irongeek.com/downloads/OSfuscate.3.zip e non necessita di installazione. In più è completamente personalizzabile mediante file di configurazione, che hanno estensione .os e contengono tutte le informazioni necessarie per imitare un particolare sistema.

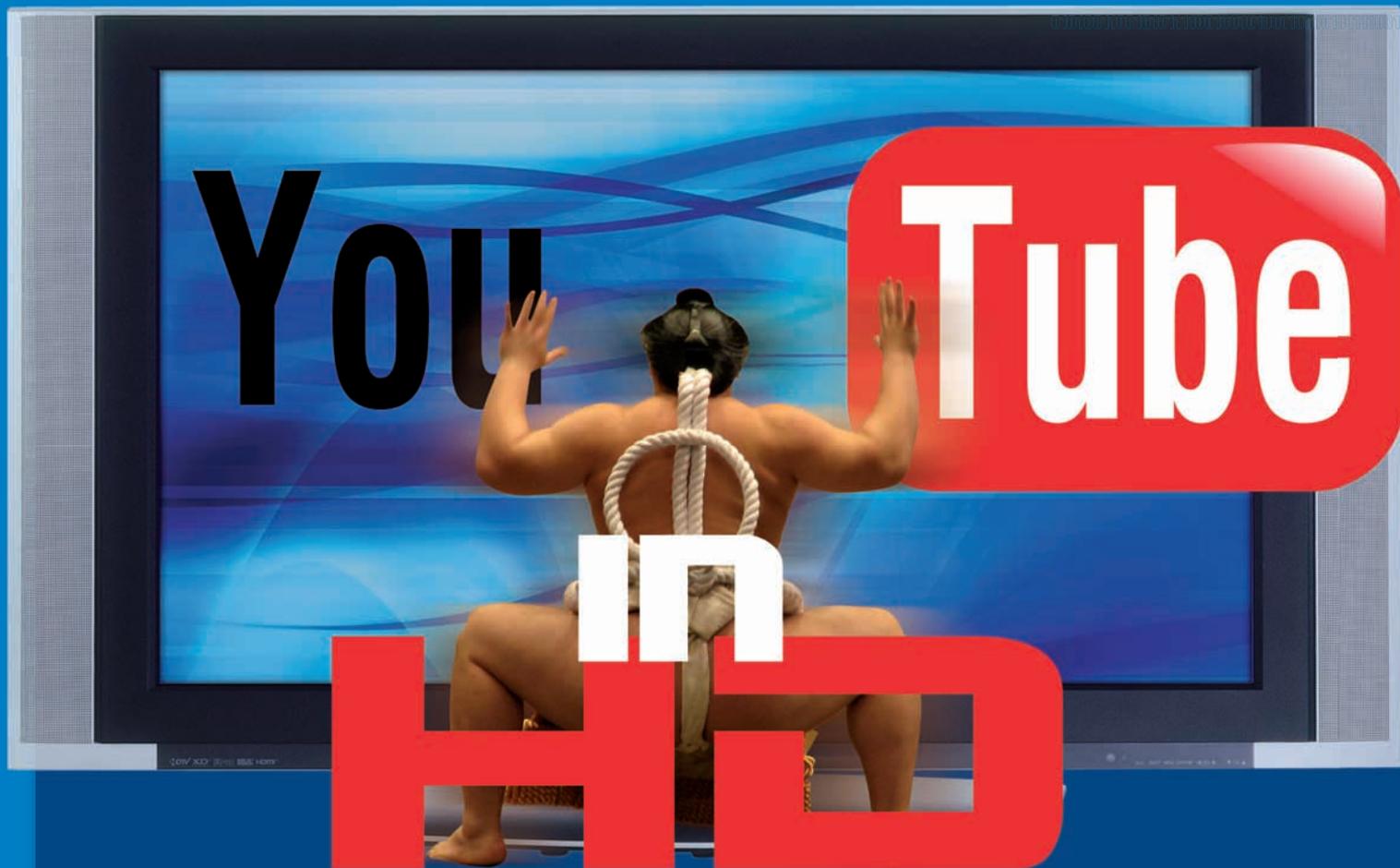
:: Ma non è finita

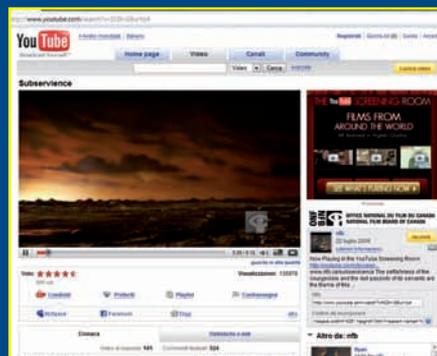
Questo operazione di offuscamento ci mette al sicuro da una scansione occasionale e non approfondita, magari condotta da programmi che si limitano alla superficie senza entrare nel dettaglio.

Dopo la "cura" OSfuscate il nostro PC va sul Web come un Nintendo Dreamcast.

NetworkMiner e Satori sono invece più ostici, perché sono in grado di rilevare il nostro sistema operativo anche dall'impronta DHCP trasmessa sulla rete.
Non è possibile cambiare tale impronta semplicemente alterando il registro in quanto la stringa è codificata in una dll di Windows (dhcpcsvc.dll). L'unica alternativa che abbiamo è quindi armarci di un editor esadecimale che funzioni da CD o floppy avviabile (non è possibile infatti modificare la libreria mentre Windows è in funzione) e andare a modificare manualmente i byte che contengono la stringa di identificazione "MSFT 5.0", rappresentati dai valori esadecimali 4d53465420352e30.

Sfruttando la firma DHCP i cattivi riescono lo stesso a trovarci.

L'autore di OSfuscate ci dà una mano anche in questo caso: nello stesso file zip troviamo infatti il programma "dhcpcsvc patcher.exe" che serve proprio a questo scopo.
È il caso però di disabilitare la funzione di ripristino del sistema di Windows, o al riavvio troveremo di nuovo la dll non modificata. Il programma copia il file originale in un nuovo file chiamato patched-dhcpcsvc.dll, che potremo rinominare e sostituire alla dll originale avviando il PC da un CD di avvio come BartPE contenente strumenti per leggere e scrivere sul file system NTFS.

Un ultimo avvertimento: ogni modifica che facciamo al nostro sistema, la facciamo a nostro rischio e pericolo. Se qualcosa andasse storto non spariamo sul giornalista (né sul programmatore di OSfuscate)!

YouTube in HD

Guardare e "embeddare" video in alta definizione

YouTube è un po' un simbolo del concetto di "Rete libera" che tutti andiamo cercando e diffondendo. Certo, alle sue spalle c'è pur sempre il colosso Google, ma è innegabile il grado di libertà digitale che questo servizio offre agli utenti del web. Anche dal punto di vista tecnologico, YouTube si è dimostrato, fin dagli albori, con una marcia in più, proponendo una soluzione per l'esecuzione dei filmati in grado di offrire buona qualità e fluidità anche nei momenti di maggior traffico. Tuttavia, negli ultimi tempi, YouTube ha mostrato un po' il fianco nel settore dell'alta definizione: le risoluzioni più elevate della canonica 320 x 240 hanno tardato a essere supportate, e molti web-concorrenti ne hanno approfittato per farsi sotto.
Il risultato? YouTube ha tentato di recuperare il terreno perduto, supportando sì i filmati in alta definizione, ma con strumenti e menu un po' confusionari. Insomma, la tecnologia di base non manca, ma accedervi non è così intuitivo come ci ha abituato il portale video di Google.

Il supporto all'alta definizione in YouTube c'è, ma non è sempre così efficace.

:: Tutto in una stringa

Per fortuna, conoscendo qualche trucchetto niente male, YouTube si proietta, con tutta la sua potenza, verso un mondo di filmati molto più gradevoli di quelli convenzionali. Un esempio veloce? L'abbiamo con quei video disponibili in diverse risoluzioni: ce ne sono moltissimi, ma spesso la risoluzione più elevata tra quelle visualizzabili non è specificata nella scheda del filmato. Insomma, capita (spesso!) che non sia presente la voce Guarda in alta qualità, che ci permetterebbe di accedere alla miglior versione di quel dato filmato.
Per gustarsela, tuttavia, ci basta aggiungere la stringa &fmt=18 alla fine dell'indirizzo URL del filmato desiderato. A questo punto, se presente, viene caricata una versione a una risoluzione maggiore, di solito a 480

La stringa &fmt=18 in azione. In questo caso, funziona alla grande!

x 360 pixel. Certo, in questo caso non si tratta di alta definizione, ma di un buon compromesso tra qualità e velocità di caricamento ed esecuzione dei filmati, che altrimenti rischiano di scattare o bloccarsi ogni tre per due.

:: Nella pagina HTML

A questo punto, viene naturale pensare che per integrare un video YouTube a una risoluzione "maggiorata", in una pagina web, è sufficiente specificare il relativo indirizzo URL nel codice HTML. O, al limite, sfruttare il codice reperibile nella finestrella Codice da incorporare, presente nella scheda del video YouTube desiderato.
In realtà le cose non stanno proprio così: per integrare il video, dobbiamo invece inserire questa porzione di codice

```
<object width=”480” height=”397”>
<param name=”movie”
value=”(INDIRIZZO
URL)&ap=%2526fmt%3D18”></param>
<param name=”wmode”
value=”window”></param>
<embed src=”(VIDEO EM-
BED URL)&ap=%2526fmt%3D18”
type=”application/x-shockwave-
flash” wmode=”window” width=”480”
height=”397”></embed></object>
```

Con l'ovvia accortezza di sostituire INDIRIZZO URL con l'indirizzo del video da integrare.

:: In HD è meglio

Come detto, questo trucchetto ci fa tastare con mano i benefici di una risoluzione video più elevata, ma ancora lontana dall'agognata alta definizione. Eppure, se la banda lo permette, esiste una tecnica simile per farci abbracciare una risoluzione davvero HD, vale a dire la 720p (meglio di niente, no?). L'unico requisito è che sia disponibile un video a questa risoluzione, che è poi la medesima che ha fatto la fortuna dello streaming su Netflix e dei servizi video on-demand di iTunes.
Anche in questo caso, per gustarci un video direttamente nella versione HD (ripetiamo che questa deve esistere a priori!), aggiungiamo all'indirizzo URL l'istruzione fmt, ma con un parametro diverso: &fmt=22. In molti casi, questa istruzione sostituisce efficacemente anche quella vista in precedenza (&fmt=18), andando comunque a caricare il video a più alta risoluzione tra quelli disponibili. E se non c'è alcuna versione "maggiorata"? Niente paura: viene caricata quella predefinita.

:: Ancora sull'embedding

Se è vero che il nostro amato trucchetto funziona perfettamente per gustarsi dei video HD direttamente su YouTube, non possiamo dire altrettanto delle classiche istruzioni HTML necessarie al "embedding" (integrazione) del filmato in alta definizione nella nostra pagina web. In questo caso, infatti, dobbiamo affidarci a un codice leggermente diverso da quello visto in precedenza:

```
<object width=”600” height=”362”>
<param name=”movie”
value=”(INDIRIZZO URL)&fs=1&rel=0&ap
=%2526fmt%3D22”></param><param
name=”allowFullScreen”
value=”true”></param>
<param name=”allowscriptaccess”
value=”always”></param>
<embed src=”(INDIRIZZO
URL)&rel=0&ap=%2526fmt%3D22”
type=”application/x-shockwave-
flash” allowscriptaccess=”always”
allowfullscreen=”true” width=”600”
height=”362”></embed>
</object>
```

Anche in questo caso, al posto di INDIRIZZO URL dobbiamo immettere l'indirizzo del video desiderato. Va da sé che i codici presentati in queste pagine vanno adattati alle nostre esigenze, e questo è particolarmente vero quando abbiamo a che fare con nostri video, caricati su YouTube. Per chi, poi, mastica codice Ajax, esiste uno script, reperibile su http://userscripts.org/scripts/show/31864 , pronto a eseguire automaticamente la versione HD di un video. E, soprattutto, con una velocità e fluidità da record. Pronti a passare all'alta definizione di YouTube?

I video HD sono strabilianti, ma richiedono una banda generosa.

Supercomputer low cost

Grande potenza di calcolo "rustic": costruiamo da soli un supercalcolatore in cluster computing

Chi ha detto che per avere grande potenza di calcolo dobbiamo spendere tanti soldi? Basta un po' di fantasia. Saper maneggiare qualche attrezzo e avere a disposizione un (relativamente) piccolo budget per costruirci in casa un supercomputer degno di un centro di calcolo professionale. Se vi state chiedendo quanti soldi, vi possiamo assicurare che spendereste di più per comprare un computer di marca progettato per i videogiochi più pesanti.
Questo è possibile grazie al cluster computing. Andremo cioè a creare un'unica unità di calcolo composta da più computer collegati tra loro sui quali, attraverso software apposito, viene distribuita l'elaborazione che ci interessa. Il tutto ovviamente verrà studiato e realizzato con un occhio al budget e uno alla praticità e alla semplicità di costruzione.

:: Corazza svedese e nel cuore il pinguino

I computer che costruiremo sono composti dai soli elementi essenziali per il loro funzionamento. Il primo problema che ci dobbiamo porre è dove sistemarli: potremmo lasciarli anche in bella vista, ma sarebbe poco pratico e poco ordinato. Con case per ogni PC spenderemmo troppo. Abbiamo una soluzione alternativa: uno schedario metallico Helmer prodotto da Ikea e venduto a meno di 30 euro, che conterrà tutto il nostro cluster. Avremo a disposizione sei cassetti, quindi sei PC che costituiranno i nodi del cluster. Nulla ci vieta di iniziare anche con un solo PC e poi a mano a mano terminare il lavoro quando abbiamo disponibilità di componenti o di soldi. In ogni cassetto trova posto tutto l'hardware necessario per un PC: una scheda madre con sezione video integrata, un processore, un disco fisso, un modulo di RAM e un alimentatore, il tutto rigorosamente low cost.
Per il sistema operativo non abbiamo dubbi: Linux è doppiamente adatto allo scopo, primo perché è completamente gratuito e altamente personalizzabile, secondo perché è più facile trovare software open source per l'implementazione di un cluster per piattaforma Linux piuttosto che per Windows o altri sistemi operativi.

:: I componenti

Innanzitutto dobbiamo decidere su quale architettura hardware vogliamo basare il sistema. Dato che vogliamo risparmiare al massimo, è meglio optare per AMD piuttosto che per Intel: la differenza di prezzo si fa sentire. Sul Web, al costo di 51 euro l'una, possiamo comprare sei

schede madri Asus M2N68-CM. Queste schede madri integrano la sezione video Nvidia e possono accogliere i più recenti processori AMD a 64 bit, quindi avremo anche margine per eventuali upgrade futuri. La CPU potrebbe essere scelta tra quelle disponibili nella linea server di AMD, ma per restare sulla stessa linea di prezzo scegliamo una AMD Athlon 64 X2 4450E da 62 euro, un dual core che comunque ci garantisce una buona potenza di calcolo e, soprattutto, consuma molto poco (tenere acceso un cluster di sei PC costa comunque in termini di energia, quindi conviene scegliere elementi che consumano poco).
La RAM e il disco fisso possiamo sceglierli in base ai nostri gusti e a quello che troviamo disponibile sul mercato. Rimanendo sotto i 50 euro a pezzo possiamo optare per le Corsair TWIN2X 2048-6400C4 EPP, una coppia di moduli da 1 gigabyte da 44 euro, e per un Seagate Barracuda 7200.10 80GB 8MB SATA-II da 39 euro. Infine, una PSU Enermax FMA II EG375AX-VE(G) da 370W e 58 euro ci fornisce abbastanza potenza per un computer minimale, dato che non dobbiamo alimentare schede aggiuntive.

Descrizione	Quantità	Prezzo €	Totale €
Ikea Helmer	1	30 €	30 €
Asus M2N68-CM	6	51 €	306 €
AMD Athlon 64 X2 4450E	6	62 €	372 €
Corsair TWIN2X 2048-6400C4 EPP	6	44 €	264 €
Seagate Barracuda 7200.10 80GB	6	39 €	234 €
Enermax FMA II EG375AX-VE(G)	6	58 €	348 €
Minuterie, HUB di rete, cavi, ecc.	1	146 €	146 €
Totale finale			€ 1.700

:: La realizzazione

La difficoltà maggiore, in questo progetto, è far stare tutto ciò che serve dentro un cassetto dello schedario.
In realtà, non avendo bisogno di molto spazio, possiamo studiare la disposizione che più ci aggrada, ma dobbiamo tenere presente due cose. Innanzitutto, la circolazione dell'aria. Gli alimentatori andranno montati sulla parte posteriore del cassetto e dovranno poter accedere all'esterno con la ventola: significa che i cassetti dovranno essere tagliati a dovere con gli strumenti adatti per dare modo all'aria calda di uscire (possiamo usare come sagoma il retro di un comune case per PC) e per avere accesso alla presa di ingresso della corrente. Anche il retro del mobile dovrà essere lasciato aperto oppure ritagliato per permettere al flusso d'aria calda di uscire. Dovremo ritagliare anche una presa d'aria anteriore, in modo che l'aria fresca possa entrare. Se desideriamo possiamo anche comprare dei LED da inserire sul pannello frontale dei cassetti per segnalare l'accensione di ogni elemento e l'attività del disco, un utile strumento di controllo. La scheda madre, ricordiamolo, deve essere distanziata dal metallo del fondo del cassetto (non c'è bisogno di dirlo, vero?).
Naturalmente il sistema operativo dovrà essere installato su tutte le macchine dopo aver collegato un monitor, una tastiera e un mouse. In seguito questi elementi non serviranno più, tutto il sistema potrà essere controllato da remoto usando il nostro computer principale.
Possiamo quindi completare la costruzione con un hub di rete almeno da 8 porte per il collegamento, una presa multipla di corrente con almeno 9 posizioni (si trovano facilmente nei mercatoni di informatica ed elettrodomestici) e siamo pronti per il passo successivo.

:: E ora il software

È importante che tutti i PC abbiano la stessa configurazione e la stessa dotazione di software.
Per il sistema operativo non sussistono particolari problemi, dobbiamo solo scegliere la distro Linux più adatta o che più ci piace. Il software di gestione del cluster e gli applicativi, invece, dipendono dall'uso che ne vogliamo fare. Su Sourceforge.net troveremo diverse implementazioni, come Beowulf, OpenSSI o MOSIX, dobbiamo solo leggerne le caratteristiche e vedere quale più si adatta alle nostre esigenze.
Già, ma quali sono queste esigenze? Dobbiamo solo scegliere. Possiamo ad esempio creare una rendering farm per la creazione di immagini e filmati 3D con software evoluti come quelli usati da Pixar o da Dreamworks per creare i loro celebri capolavori di animazione degli ultimi anni, oppure una Web farm per ospitare i siti Web che creeremo. O semplicemente usare il mega-PC così come è, un supercomputer velocissimo e potente. Dopotutto, abbiamo a disposizione la potenza di ben 12 processori, non dimentichiamolo!

Privateer

SEI DI LINUX O DI UN ALTRO PIANETA?

Venti domande la cui risposta ti sorprenderà e qualche altra cosa che ti era sfuggita

Se non sai che cos'è Linux... atterra. Un vero hacker inizia da Windows, nel 90 percento dei casi, per pure ragioni statistiche: il 90 percento dei computer è Windows. Il vero hacker scappa da Windows appena è possibile, perché il vero padrone del computer usa Unix e Linux è una variante di Unix, open source (quelli bravi lo modificano a piacere e poi pubblicano le modifiche in modo che tutti ne possano approfittare) e gratuita (un computer può costare soldi, ma la conoscenza deve essere a disposizione di tutti).

Di Linux è facile sapere le cose facili: si srive qualcosa su Google e qualcosa viene fuori. Le cose difficili, invece, come si sanno? Ma facendo il nostro test! Vediamo quanto siete bravi e quanti punti riuscite a fare. Il voto perfetto non sarà facile come a scuola, dove oramai i professori sono più asini di quelli cui insegnano...

01 Quale di queste aziende non ha mai avuto una propria versione di Linux?

- Apple
- SCO Group
- Sun Microsystems
- IBM

02 Perché usare grub al posto di lilo?

- Per chiamare il cane di casa con un nome più aggressivo
- Per poter fare il boot via rete
- Per poter scegliere se fare partire Windows o Linux
- Per supportare più di quattro gigabyte di Ram

03 Quale di questi pacchetti NON aiuta a usare programmi Windows su Linux?

- CrossOver Office
- Mono
- Samba
- VMware

04 Che cosa si intende per shebang?

- Un altro modo di dire Ctrl-Alt-Del
- Un transessuale che vince l'Isola dei famosi
- Una sequenza di caratteri che indica l'inizio di uno script
- Una parolaccia beneaugurante da dire quando si cambia la partizione di Windows per fare posto a Linux

05 Quale di queste distro Linux è diversa dalle altre?

- FedoraCore
- CentOS
- Novell Suse Linux Enterprise
- Oracle Enterprise Linux

06 Quale di questi kernel Linux è più stabile su hardware supportato?

- 2.3
- 2.4
- 2.5
- 2.7

07 Che cosa distingue l'installazione di Gentoo Linux dalle altre?

- Ha un installatore avanzato, grafico, amichevole
- Durante l'installazione suona musica hip-hop
- Compila al volo da codice sorgente e quindi è sempre ottimizzato
- Installa sia Linux che Windows sulla stessa partizione

08 Quale di queste aziende NON ha pubblicato driver open source per il proprio hardware grafico?

- ATI/AMD
- Intel
- Nvidia
- Via

09 Che cos'è SELinux?

- Un ambiente che somiglia a Linux e si installa sotto Windows
- Un set di modifiche al kernel Linux sviluppato dalla National Security Agency americana
- Una distro Linux per netbook e smartphone
- Una vecchia morosa di Harry Potter

10 Quale sistema di controllo versione si usa per contribuire alla programmazione del kernel Linux?

- Subversion
- CVS
- BitKeeper
- git

11 Quante righe di C++ contiene approssimativamente l'albero dei sorgenti di Linux?

- Meno di 500 mila
- Circa un milione
- Tra due e quattro milioni
- Più di quattro milioni

12 Quale di questi programmatori non ha mai donato codice sorgente al kernel di Linux?
- Hans Reiser
- Linus Torvalds
- Richard Stallman
- Eric Raymond

13 Quale filesystem offre le migliori prestazioni con file multimediali molto molto molto grossi?
- FAT32
- ReiserFS 3
- XFS
- Ext2fs

14 Quale di questi sistemi di gestione finestre viene usato più spesso su Linux?
- Gnome
- KDE
- Enlightenment
- X.org

15 A che server montare filesystem Linux con l'opzione noatime?
- A migliorare le prestazioni grazie a una minore frequenza delle scritture su disco
- A montare una partizione in sola lettura
- A usare una parola che gli amici non conoscono di cui ci possiamo vantare
- A montare partizioni Windows su un computer Linux

16 Quale di queste tecnologie di virtualizzazione consente di fare funzionare macchine virtuali Windows su Linux?
- OpenVZ
- Linux-VServer
- Xen
- Hyper-V

17 Nel gergo Linux, che cos'è un blob binario?
- L'unità di misura standard dello spazio di swap del kernel
- Un driver caricato nel kernel come oggetto binario, per il quale non è disponibile codice sorgente
- Un file orfano di cui la tabella di allocazione di sistema ha perso le tracce sul disco
- Uno che non si stacca mai dal computer e continua a mangiare merendine

18 Quale di queste distro Linux NON basa l'installazione su pacchetti RPM?
- Red Hat Enterprise Linux
- Novell Suse Linux Enterprise
- Ubuntu
- Mandriva

19 Quale di queste è tra le prime dieci aziende che contribuiscono allo sviluppo del kernel Linux?
- Intel
- Google
- HP
- Cisco

20 (whew!): chi è Larry Ewing?
- Un personaggio della soap opera Dallas
- L'uomo che ha inviato più patch per mettere a punto il kernel Linux
- Uno pseudonimo di Linus Torvalds
- Il creatore di Tux, la mascotte ufficiale di Linux

David Nool

RISPOSTE PUNTEGGI E INSULTI

01 IBM. È un'azienda che supporta tantissimo Linux, ma non ne ha mai fatto una sua versione.
02 Per fare il boot via rete, cosa che lilo, sempre valido ma un po' antico, non fa.
03 Samba. È indispensabile per fare rete tra computer Linux e Windows, ma non per usare programmi Windows su Linux.
04 Una sequenza unica di caratteri che indica l'inizio di uno script. In Unix i programmatori abbreviano così "shell bang": un cancelletto (#) seguito da un punto esclamativo (!), quest'ultimo detto"bang".
05 Novell Suse Linux Enterprise. Le altre basano il codice sorgente su quello di Red Hat; Suse invece va per conto proprio.
06 2.4. Le versioni dispari sono sempre considerate di sviluppo e instabili. La 2.7 non esiste neanche. L'unica versione stabile nella lista è la 2.4.
07 Compila al volo da codice sorgente e quindi è sempre ottimizzato. Gentoo ci mette una vita a installarsi, ma è l'installazione ad hoc per il nostro PC.
08 Nvidia. Sono cattivi; tutti gli altri hanno driver open source per le loro schede video.
09 Un set di modifiche al kernel Linux sviluppato dalla National Security Agency americana, che serve per rafforzare la sicurezza di Linux in modo da soddisfare le specifiche del governo USA. A quel punto però è meglio usare OpenBSD.
10 git. Linus Torvalds, il fondatore di Linux, voleva usare BitKeeper, ma un po' di collaboratori si facevano problemi di licenza. Allora ha creato un sistema apposta.
11 Meno di 500 mila. Linus Torvalds non è un entusiasta di C++ e così il 99,71 percento del sorgente di Linux è C standard, non C++.
12 Richard Stallman. Stallman pensa che il nome dovrebbe essere GNU/Linux, perché Linux da solo non sarebbe un sistema operativo completo senza l'ausilio di codice sviluppato dalla Free Software Foundation nell'ambito del progetto GNU. E Stallman non ha mai contribuito al kernel.
13 XFS. Chi non ci crede, provi. Lo ha creato Silicon Graphics apposta per lavorare su grossi file multimediali.
14 X.org. Domanda trappola! Solo X.org è un sistema di gestione finestre. Gli altri sono interfacce grafiche appoggiate su X.org.
15 A migliorare le prestazioni grazie a una minore frequenza delle scritture su disco. Di solito Linux aggiorna il time stamp di un file (data e ora di modifica) tutte le volte che vi si accede.
16 Xen. Se il nostro processore supporta la tecnologia VT di Intel o AMD-V di AMD, naturalmente. Ma Xen permette di attivare macchine virtuali Windows; gli altri, solo Linux.
17 U-n driver caricato nel kernel come oggetto binario, per il quale non è disponibile codice sorgente. Succede quando il fornitore del driver si rifiuta di renderlo open source. Parte della comunità trova questa situazione discutibile, ma a volte è l'unico modo di fare funzionare qualcosa.
18 Ubuntu. Ubuntu nasce da Debian, che ha il proprio sistema di distribuzione. Le altre, da Red Hat.
19 Intel. Ha fornito più del quattro percento delle modifiche al kernel.
20 il creatore di Tux, la mascotte ufficiale di Linux. Larry ha disegnato il pinguino più simpatico del mondo nel 1996, per una versione di GIMP.

CONTA LE RISPOSTE E POI CONTROLLA IL RISULTATO DEL TEST!

Da zero a cinque risposte esatte: Acquacedratario. Non sei un caso disperato, ma devi ancora scoprire le bellezze di Linux. Leggi HJ e scaricati almeno un CD Live, così inizi a renderti conto.

Più di cinque e fino a dieci risposte esatte: Sarchiapone. Non esitare ulteriormente e programma l'installazione di Linux; quel Windows penoso e trasudante virus diventerà presto un ricordo. Leggi HJ e fai tesoro di tutti i suoi consigli.

Più di dieci e fino a quindici risposte esatte: Conestabile. Ti manca solo l'ultimo passo: eliminare l'installazione di Windows. Linux ha proprio tutto quello che serve per fare quello che vuoi e oltretutto scopri sempre cose nuove e interessanti. Leggi HJ e stai pensando di scrivere un articolo su Linux. Beh, fallo. Sarà ottimo!

Da quindi a venti risposte esatte: Icositetraedro. Vivi dentro Linux meglio di un tamarro in discoteca, e ha davanti a te un futuro informatico luminoso. Continua a mandarci articoli su Linux, ma ogni tanto riposati! Complimenti veri.

Il sito web in tasca!

Come installare un sito web sul proprio cellulare accessibile da internet

Un sito web si basa su alcuni punti cardine per funzionare: è disponibile online, è rintracciabile e ha dei contenuti fruibili tramite browser. Chiunque voglia avere il proprio sito deve quindi rivolgersi a un provider che gli renda disponibile lo "spazio Web" dove collocare i contenuti e si occupi della gestione della macchina che fisicamente ospita tali contenuti. Per funzionare, il sito Web si appoggia a un server http e il prodotto open source più famoso al mondo è Apache.

::RACCOON & MOBILE WEB SERVER

Grazie a Nokia è disponibile da qualche tempo un porting di Apache per la nota piattaforma Symbian, utilizzata su molti dei suoi telefonini, che è stato chiamato Raccoon. Ne è stata realizzata anche una versione commerciale chiamata Mobile Web Server (MWS), che offre svariati servizi che spaziano dalla condivisione di contenuti multimediali ai blog (wiki.opensource.nokia.com/projects/Mobile_Web_Server). La prima versione però, oltre a essere completamente open source, permette di scrivere moduli personalizzati per Apache, cosa non permessa con MWS.
Installare Raccoon (o MWS) sul proprio telefonino non prescinde comunque dai punti cardine già menzionati.

La memoria del telefonino diventerà lo spazio Web (hosting), ma si aggiunge una ulteriore difficoltà: dovremo poterci connettere a Internet, tramite WLAN o reti cellulari; in questo secondo caso (oltre a necessitare di una tariffa flat o semi-flat) scopriremo che il nostro gestore blocca le connessioni dati entranti da Internet e dirette al terminale.

:: AGGIRARE IL BLOCCO

Per superare questa limitazione è necessario sfruttare il meccanismo di Network Address Traslation (NAT). Questo permette a un terminale posto dietro un firewall di essere raggiunto dall'esterno (proprio come nel nostro caso) ma occorre un secondo terminale connesso a Internet che funga da gateway per il primo. All'interno di Raccoon è stato integrato un client VPN che permette il routing tra il server posto sul telefonino e il gateway. Fino a qualche mese fa Nokia forniva un servizio di gateway completamente gratuito, cui era possibile registrarsi e accedere tramite l'invio di una mail ma con il rilascio di MWS sono state sospese le nuove iscrizioni, limitando l'iscrizione libera ai soli utenti di MWS (e il gateway di MWS utilizza un protocollo diverso da quello di Raccoon). L'alternativa per usare comunque Raccoon è quella di scaricare un altro pacchetto software, chiamato Raccoon Gateway, che realizza su un PC con-

nesso a Internet lo stesso servizio che veniva offerto online da Nokia (**sourceforge.net/project/showfiles.php?group_id=167580&package_id=222728**). L'ultima release disponibile è la 0.6.3.
Raccoon Gateway viene rilasciato in forma di sorgente e per la compilazione suggeriamo caldamente Linux (su Windows va installato Cygwin e vanno copiati diversi file in più locazioni), dato che gli script già pronti sono pensati per un ambiente Unix-like. Sono inoltre richiesti JDK 1.5.x, MySQL 3.1.x & Java Connector, Tomcat 5.5.x già installati, svariate librerie Java (da MyFaces) e tool di compilazione (ant, mmake). Nulla vieta di utilizzare una macchina virtuale. Per le prove abbiamo utilizzato una Debian 4.0 con Virtual PC su un notebook con XP.

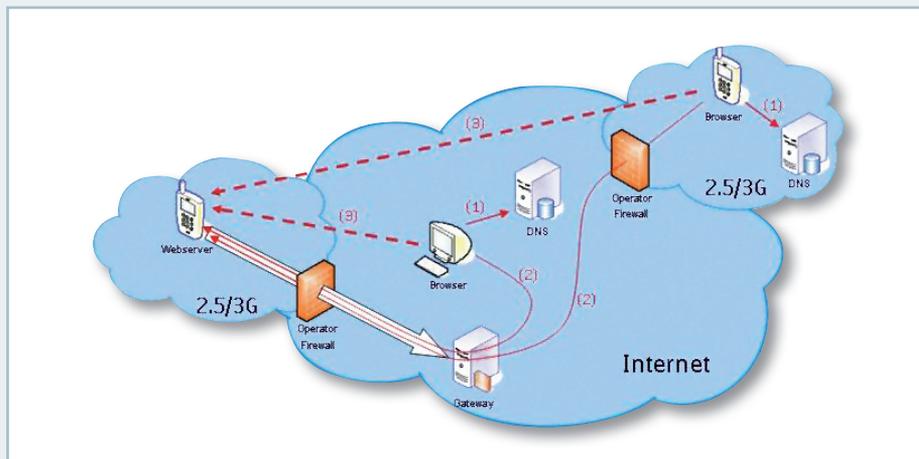
:: IL GATEWAY (RACCOON SERVER)

Purtroppo la compilazione di tutto il pacchetto sembra un'opera infinita: sono infatti molti i punti da risolvere prima di avere un ambiente correttamente configurato per l'elaborazione dei sorgenti. Una volta compilati, sono necessari diversi test per verificare che le varie componenti Web, Java e architettura server/client del gateway comunichino tra loro correttamente. Aggiungiamo il fatto che, dal momento che il prodotto non viene più sviluppato (ed è abbastanza di nicchia), manca il supporto tipico dei forum open source.
Infine è necessario modificare il codice che realizza la configurazione del database, nel file scriviamo:

```
<raccoon gw dir>/db/src/com/nokia/
mws/db/DbMgr.java
-- ho sostituito la linea
"cmd = Command.valueOf(args[0]);"
-- con
"cmd = Command.create;"
```

per forzare la creazione del file **mws-gw-db.cfg** e sbloccare il resto della compilazione, in quanto lo script non riconosce correttamente il comando "create" da linea di comando.
Una volta terminati i test con esito positivo, ci si ritova sulla stessa macchina sia l'applicazione lato server sia l'applicazione lato client che simula il telefonino. A questo punto è possibile lanciare il Connector lato server e testare con un browser la connessione in locale verso **http://127.0.0.1:8080**; se questa prova va a buon fine, il gateway è pronto ed è possibile testare la connessione con il telefonino)!
Compilato e lanciato Raccoon Gateway, vanno verificati i seguenti passaggi:

- il PC dove gira il gateway deve essere connesso a Internet;
- l'eventuale firewall presente deve permettere di ricevere connessioni dall'esterno verso la porta associata al Connector (di default la **15001**);
- l'indirizzo IP pubblico con il quale il PC esce su Internet sarà il gateway nel telefonino.

locale: in **Menu→Settings**, impostare Portal su 0.0.0.0 e Portal port su 0, lasciando inalterati gli altri valori; poi nel menu selezionare **"Start w/o Connector"** che avvia il server Web senza connettere il telefonino al gateway. Se non è stato cambiato l'indirizzo del server, sarà possibile aprire la pagina **http://127.0.0.1** con il browser Web del telefonino per vedere un messaggio di benvenuto di Apache.
Con il gateway correttamente funzionante, impostiamo in **Raccoon→Menu→Settings** i valori di user, password e porta del server scelti nella configurazione del gateway.
Come indirizzo "gateway" andrà invece inserito l'indirizzo IP pubblico attualmente in uso dal PC. A questo punto selezionare **Menu→Start Connector** e, se tutto fila liscio, riusciremo a vedere la pagina di benvenuto di TomCat!
Ora è possibile definire un nome utente cui è associato lo spazio Web

:: RACCOON SUL TELEFONINO

Raccoon viene tuttora manutenuto, ma è reso disponibile solo per la 3a edizione di Symbian (http://sourceforge.net/projects/raccoon). Prima di tutto va installato Python per Symbian (**http://opensource.nokia.com/projects/pythonfors60**), poi vanno installati i tre pacchetti .sis contenuti nell'archivio di Raccoon: raccoon, httpdconf, webcontent.

A questo punto è possibile lanciare Raccoon (nel menu principale) e verificare il corretto funzionamento in che andremo a rendere visibile su Internet. Per le prime prove è già esistente l'utente jim.id ed è possibile puntare al suo spazio Web andando all'indirizzo **http://<ip gateway>/~jim.hacker** (jim.hacker è l'utente registrato nel database di partenza associato allo user **jim.id**). Questo sarà l'indirizzo pubblico per raggiungere poi il nostro telefonino; in caso di server raccoon offline, viene visualizzato un messaggio di cortesia, altrimenti la richiesta viene reindirizzata verso il terminale cconnesso (tramite "connector", id e password) al gateway.

Massimiliano Brasile